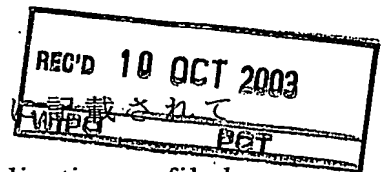


22.08.03

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.



出 願 年 月 日
Date of Application: 2002年 9月25日

出 願 番 号
Application Number: 特願2002-278436
[ST. 10/C]: [JP2002-278436]

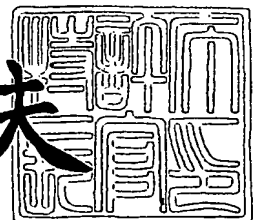
出 願 人
Applicant(s): ソニー株式会社

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

2003年 9月26日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫



BEST AVAILABLE COPY

【書類名】 特許願

【整理番号】 0290539407

【提出日】 平成14年 9月25日

【あて先】 特許庁長官殿

【国際特許分類】 E05B 49/00
G08B 23/00

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 油井 康二

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 松村 広幸

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 八重樫 章

【特許出願人】

【識別番号】 000002185

【氏名又は名称】 ソニー株式会社

【代理人】

【識別番号】 100091546

【弁理士】

【氏名又は名称】 佐藤 正美

【電話番号】 03-5386-1775

【手数料の表示】

【予納台帳番号】 048851

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9710846

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 通信装置、通信システム、制御装置および認証装置

【特許請求の範囲】

【請求項 1】

同一のものが存在しないように一元管理されて割り振られた識別情報を記憶する記憶部と、

ドアの施錠、開錠を行なうためのドアロック機構を制御するための制御装置との通信を行なう通信部と、

前記通信部を介して、前記記憶部の前記識別情報を、前記ドアの施錠、開錠を制御するための電子鍵情報として、前記制御装置に送信するように制御する制御部と、

を備える通信装置。

【請求項 2】

IC (Integrated Circuit ; 集積回路) カードからなることを特徴とする請求項 1 に記載の通信装置。

【請求項 3】

前記制御装置との通信機能ではない主たる別機能を備える電子機器からなることを特徴とする請求項 1 に記載の通信装置。

【請求項 4】

電子鍵情報に応じてドアの施錠、開錠を行なうためのドアロック機構を制御する制御装置と、前記制御装置に前記電子鍵情報を送信する通信装置とからなる通信システムであって、

前記通信装置は、

同一のものが存在しないように一元管理されて割り振られた識別情報を記憶する第 1 の記憶部と、

前記制御装置との通信を行なうための第 1 の通信部と、

前記第 1 の通信部を介して、前記第 1 の記憶部の前記識別情報を、前記ドアの施錠、開錠を制御するための電子鍵情報として、前記制御装置に送信するように制御する第 1 の制御部と、

を備え

前記制御装置は、

前記通信装置と通信を行なうための第2の通信部と、

前記識別情報を前記電子鍵情報として記憶する第2の記憶部と、

前記第2の記憶部に前記識別情報を前記電子鍵情報として登録するための登録手段と、

前記第2の通信部を通じて前記通信装置から受信した前記識別情報と、前記第2の記憶部に記憶されている識別情報とを比較し、その比較結果に基づいて前記ドアの施錠、開錠を制御する第2の制御部と、

を備えることを特徴とする通信システム。

【請求項5】

請求項4に記載の通信システムにおいて、

前記制御装置の前記第2の記憶部には、前記電子鍵情報としての前記識別情報は、複数個、登録されて記憶可能とされる

ことを特徴とする通信システム。

【請求項6】

請求項5に記載の通信システムにおいて、

前記複数個の識別情報は、本鍵情報と、バックアップ鍵情報とからなる

ことを特徴とする通信システム。

【請求項7】

請求項6に記載の通信システムにおいて、

前記第2の制御部は、前記第2の通信部を通じて前記通信装置から受信した前記識別情報と、前記第2の記憶部に記憶されている前記本鍵情報としての識別情報とを比較し、その比較結果に基づいて前記ドアの施錠、開錠を制御する

ことを特徴とする通信システム。

【請求項8】

請求項7に記載の通信システムにおいて、

前記制御装置は、前記第2の記憶部の前記本鍵情報として登録されている識別情報が抹消されたときに、前記バックアップ鍵情報として登録されている識別情

報を本鍵情報として扱う

ことを特徴とする通信システム。

【請求項 9】

請求項 6 に記載の通信システムにおいて、

前記第 2 の制御部は、前記第 2 の通信部を通じて前記通信装置から受信した前記識別情報と、前記第 2 の記憶部に記憶されている前記本鍵情報および前記バックアップ鍵情報としての識別情報とを比較し、その比較結果に基づいて前記ドアの施錠、開錠を制御する

ことを特徴とする通信システム。

【請求項 10】

電子鍵情報に応じてドアの施錠、開錠を行なうためのドアロック機構を制御するドアロック制御装置と、前記電子鍵情報の認証を行なう認証装置と、前記電子鍵情報を前記ドアロック制御装置または前記認証装置に送信する通信装置とからなる通信システムであって、

前記通信装置は、

同一のものが存在しないように一元管理されて割り振られた識別情報を記憶する第 1 の記憶部と、

前記制御装置との通信を行なうための第 1 の通信部と、

前記通信部を介して、前記記憶部の前記識別情報を、前記ドアの施錠、開錠を制御するための電子鍵情報として、前記制御装置に送信するように制御する第 1 の制御部と、

を備え

前記ドアロック制御装置は、

前記通信装置と通信を行なうための第 2 の通信部と、

前記第 2 の通信部で受信した前記通信装置からの前記電子鍵情報としての前記識別情報を前記認証装置に転送する転送手段と、

前記認証装置からの前記電子鍵情報についての認証結果を受信する手段と、

前記受信した前記認証結果に基づいて、前記ドアの施錠、開錠を制御する第 2 の制御部と、

を備え、
前記認証装置は、
前記電子鍵情報としての前記識別情報を記憶する第 2 の記憶部と、
前記第 2 の記憶部に前記識別情報を電子鍵情報として記憶して登録するための登録手段と、

前記ドアロック制御装置から転送されてくる前記識別情報と、前記第 2 の記憶部に記憶されている識別情報とを比較し、その比較結果を前記電子鍵情報の認証結果として前記ドアロック制御装置に送る手段と、

を備えることを特徴とする通信システム。

【請求項 11】

請求項 10 に記載の通信システムにおいて、
前記認証装置の前記登録手段は、前記転送手段により前記ドアロック制御装置から送られてくる識別情報を、前記電子鍵情報として前記第 2 の記憶部に記憶して登録する

ことを特徴とする通信システム。

【請求項 12】

請求項 10 に記載の通信システムにおいて、
前記認証装置は、さらに前記通信装置と通信を行なうための第 3 の通信部を備え、

前記認証装置の前記登録手段は、前記第 3 の通信部を通じて前記通信装置から送られてくる識別情報を、前記電子鍵情報として前記第 2 の記憶部に記憶して登録する

ことを特徴とする通信システム。

【請求項 13】

請求項 10 に記載の通信システムにおいて、
前記認証装置の前記第 2 の記憶部には、前記電子鍵情報としての前記識別情報は、複数個、登録されて記憶可能とされる

ことを特徴とする通信システム。

【請求項 14】

請求項 13 に記載の通信システムにおいて、
前記複数の識別情報は、本鍵情報と、バックアップ鍵情報とからなる
ことを特徴とする通信システム。

【請求項 15】

請求項 14 に記載の通信システムにおいて、
前記認証装置では、前記ドアロック制御装置から受信した前記識別情報と、前
記第 2 の記憶部に記憶されている前記本鍵情報としての識別情報とを比較し、そ
の比較結果を認証結果とする
ことを特徴とする通信システム。

【請求項 16】

請求項 15 に記載の通信システムにおいて、
前記認証装置は、前記第 2 の記憶部の前記本鍵情報として登録されている識別
情報が抹消されたときに、前記バックアップ鍵情報として登録されている識別情
報を本鍵情報として扱う
ことを特徴とする通信システム。

【請求項 17】

請求項 14 に記載の通信システムにおいて、
前記認証装置は、前記ドアロック制御装置から受信した前記識別情報と、前記
第 2 の記憶部に記憶されている前記本鍵情報および前記バックアップ鍵情報とし
ての識別情報とを比較し、その比較結果を認証結果とする
ことを特徴とする通信システム。

【請求項 18】

同一のものが存在しないように一元管理されて割り振られた識別情報を、電子
鍵情報として記憶するための記憶部と、
前記識別情報を受信するための通信部と、
前記記憶部に前記識別情報を前記電子鍵情報として登録するための登録手段と
、
前記通信部を通じて受信した前記識別情報と、前記第 2 の記憶部に記憶されて
いる識別情報とを比較し、その比較結果に基づいてドアの施錠、開錠を制御する

制御部と、

を備えることを特徴とする制御装置。

【請求項 19】

請求項 18 に記載の制御装置において、

前記記憶部には、前記電子鍵情報としての前記識別情報は、複数個、登録されて記憶可能とされる

ことを特徴とする制御装置。

【請求項 20】

請求項 19 に記載の制御装置において、

前記複数個の識別情報は、本鍵情報と、バックアップ鍵情報とからなることを特徴とする制御装置。

【請求項 21】

請求項 20 に記載の制御装置において、

前記制御部は、前記通信部を通じて受信した前記識別情報と、前記記憶部に記憶されている前記本鍵情報としての識別情報とを比較し、その比較結果に基づいて前記ドアの施錠、開錠を制御する

ことを特徴とする制御装置。

【請求項 22】

請求項 21 に記載の制御装置において、

前記記憶部の前記本鍵情報として登録されている識別情報が抹消されたときに、前記バックアップ鍵情報として登録されている識別情報を本鍵情報として扱うことを特徴とする制御装置。

【請求項 23】

請求項 20 に記載の制御装置において、

前記制御部は、前記通信部を通じて受信した前記識別情報と、前記記憶部に記憶されている前記本鍵情報および前記バックアップ鍵情報としての識別情報とを比較し、その比較結果に基づいて前記ドアの施錠、開錠を制御する

ことを特徴とする制御装置。

【請求項 24】

同一のものが存在しないように一元管理されて割り振られた識別情報を電子鍵情報として記憶する記憶部と、

前記記憶部に前記識別情報を電子鍵情報として記憶して登録するための登録手段と、

ドアの施錠、開錠を制御するようにする制御装置から送られてくる前記識別情報を受信する受信手段と、

前記受信手段で受信した前記制御装置から送られてくる前記識別情報と、前記第2の記憶部に記憶されている識別情報とを比較し、その比較結果を前記電子鍵情報の認証結果として前記制御装置に送る手段と、

を備えることを特徴とする認証装置。

【請求項 25】

請求項 24 に記載の認証装置において、

前記登録手段は、前記制御装置から送られてくる前記識別情報を、前記記憶部に記憶して前記電子鍵情報を登録する

ことを特徴とする認証装置。

【請求項 26】

請求項 24 に記載の認証装置において、

前記識別情報を受信するための別の通信部を備え、

前記登録手段は、前記別の通信部を通じて受信する識別情報を、前記電子鍵情報として前記記憶部に記憶して登録する

ことを特徴とする認証装置。

【請求項 27】

請求項 24 に記載の認証装置において、

前記記憶部には、前記電子鍵情報としての前記識別情報は、複数個、登録されて記憶可能とされる

ことを特徴とする認証装置。

【請求項 28】

請求項 24 に記載の認証装置において、

前記記憶部には、前記電子鍵情報としての前記識別情報は、複数個、登録され

て記憶される

ことを特徴とする認証装置。

【請求項 29】

請求項 28 に記載の認証装置において、

前記複数個の識別情報は、本鍵情報と、バックアップ鍵情報とからなることを特徴とする認証装置。

【請求項 30】

請求項 29 に記載の認証装置において、

前記制御装置から受信した前記識別情報と、前記記憶部に記憶されている前記本鍵情報としての識別情報とを比較し、その比較結果を認証結果とすることを特徴とする認証装置。

【請求項 31】

請求項 30 に記載の認証装置において、

前記記憶部の前記本鍵情報として登録されている識別情報が抹消されたときに、前記バックアップ鍵情報として登録されている識別情報を本鍵情報として扱うことを特徴とする認証装置。

【請求項 32】

請求項 29 に記載の認証装置において、

前記認証装置は、前記制御装置から受信した前記識別情報と、前記記憶部に記憶されている前記本鍵情報および前記バックアップ鍵情報としての識別情報とを比較し、その比較結果を認証結果とすることを特徴とする認証装置。

【請求項 33】

電子鍵情報に応じてドアの施錠、開錠を行なうためのドアロック機構を制御する制御装置と、前記制御装置に前記電子鍵情報を送信する通信装置と、前記電子鍵情報を管理するサーバ装置とからなる通信システムであって、

前記通信装置は、

同一のものが存在しないように一元管理されて割り振られた識別情報を記憶する第 1 の記憶部と、

前記制御装置との通信を行なうための第 1 の通信部と、
前記通信部を介して、前記記憶部の前記識別情報を、前記ドアの施錠、開錠を制御するための電子鍵情報として、前記制御装置に送信するように制御する第 1 の制御部と、
を備え、
前記制御装置は、
前記通信装置と通信を行なうための第 2 の通信部と、
前記サーバ装置と通信を行なうための第 3 の通信部と、
前記電子鍵情報としての前記識別情報を記憶する第 2 の記憶部と、
前記第 3 の通信部を通じて前記サーバ装置から受信した前記識別情報を前記第 2 の記憶部に前記電子鍵情報として記憶して登録するための登録手段と、
前記第 2 の通信部を通じて前記通信装置から受信した前記識別情報と、前記第 2 の記憶部に記憶されている識別情報とを比較し、その比較結果に基づいて前記ドアの施錠、開錠を制御する第 2 の制御部と、
を備え、
前記サーバ装置は、
前記通信装置の前記第 1 の記憶部に記憶されている識別情報を電子鍵情報として、前記制御装置を指定する情報とともに受信する受信手段と、
前記受信手段で受信した前記識別情報を、前記指定された前記制御装置の識別用情報と対応付けて記憶する第 3 の記憶部と、
前記受信手段で受信した前記識別情報を、前記指定された前記制御装置に転送する転送手段と、
を備えることを特徴とする通信システム。

【請求項 34】

請求項 33 に記載の通信システムにおいて、
前記サーバ装置の第 3 の記憶部および前記制御装置の第 2 の記憶部には、前記電子鍵情報としての前記識別情報は、複数個、登録されて記憶可能とされることを特徴とする通信システム。

【請求項 35】

請求項 3 4 に記載の通信システムにおいて、
前記複数の識別情報は、本鍵情報と、バックアップ鍵情報とからなる
ことを特徴とする通信システム。

【請求項 3 6】

請求項 3 5 に記載の通信システムにおいて、
前記制御装置の前記第 2 の制御部は、前記第 2 の通信部を通じて前記通信装置
から受信した前記識別情報と、前記第 2 の記憶部に記憶されている前記本鍵情報
としての識別情報とを比較し、その比較結果に基づいて前記ドアの施錠、開錠を
制御する
ことを特徴とする通信システム。

【請求項 3 7】

請求項 3 6 に記載の通信システムにおいて、
前記制御装置は、前記サーバ装置からの本鍵情報の抹消登録要求を受けたとき
に、前記第 2 の記憶部の前記本鍵情報として登録されている識別情報を抹消し、
前記バックアップ鍵情報として登録されている識別情報を本鍵情報として扱う
ことを特徴とする通信システム。

【請求項 3 8】

請求項 3 5 に記載の通信システムにおいて、
前記制御装置の前記第 2 の制御部は、前記第 2 の通信部を通じて前記通信装置
から受信した前記識別情報と、前記第 2 の記憶部に記憶されている前記本鍵情報
および前記バックアップ鍵情報としての識別情報とを比較し、その比較結果に基
づいて前記ドアの施錠、開錠を制御する
ことを特徴とする通信システム。

【請求項 3 9】

請求項 3 3 に記載の通信システムにおいて、
前記制御装置と前記サーバ装置とは、通信ネットワークを通じて接続されてお
り、前記サーバ装置には、複数の前記制御装置の前記ネットワーク上のアドレス
情報が記憶されている
ことを特徴とする通信システム。

【請求項 40】

電子鍵情報に応じてドアの施錠、開錠を行なうためのドアロック機構を制御するドアロック制御装置と、前記電子鍵情報の認証を行なう認証装置と、前記電子鍵情報を前記ドアロック制御装置または前記認証装置に送信する通信装置と、前記電子鍵情報を管理するサーバ装置とからなる通信システムであって、

前記通信装置は、

同一のものが存在しないように一元管理されて割り振られた識別情報を記憶する第1の記憶部と、

前記制御装置との通信を行なうための第1の通信部と、

前記通信部を介して、前記記憶部の前記識別情報を、前記ドアの施錠、開錠を制御するための電子鍵情報として、前記制御装置に送信するように制御する第1の制御部と、

を備え

前記ドアロック制御装置は、

前記通信装置と通信を行なうための第2の通信部と、

前記第2の通信部で受信した前記通信装置からの前記電子鍵情報としての前記識別情報を前記認証装置に転送する転送手段と、

前記認証装置からの前記電子鍵情報についての認証結果を受信する手段と、

前記受信した前記認証結果に基づいて、前記ドアの施錠、開錠を制御する第2の制御部と、

を備え、

前記認証装置は、

前記電子鍵情報としての前記識別情報を記憶する第2の記憶部と、

前記サーバ装置と通信を行なうための第3の通信部と、

前記第3の通信部を通じて前記サーバ装置から受信した前記識別情報を前記第2の記憶部に電子鍵情報として記憶して登録するための登録手段と、

前記ドアロック制御装置から転送されてくる前記識別情報と、前記第2の記憶部に記憶されている識別情報とを比較し、その比較結果を前記電子鍵情報の認証結果として前記ドアロック制御装置に送る手段と、

を備え、

前記サーバ装置は、

前記通信装置の前記第 1 の記憶部に記憶されている識別情報を電子鍵情報として、前記制御装置を指定する情報とともに受信する受信手段と、

前記受信手段で受信した前記識別情報を、前記指定された前記認証装置の識別用情報と対応付けて記憶する第 3 の記憶部と、

前記受信手段で受信した前記識別情報を、前記指定された前記認証装置に転送する転送手段と、

を備えることを特徴とする通信システム。

【請求項 4 1】

請求項 4 0 に記載の通信システムにおいて、

前記認証装置の前記第 2 の記憶部には、前記電子鍵情報としての前記識別情報は、複数個、登録されて記憶可能とされる

ことを特徴とする通信システム。

【請求項 4 2】

請求項 4 1 に記載の通信システムにおいて、

前記複数個の識別情報は、本鍵情報と、バックアップ鍵情報とからなることを特徴とする通信システム。

【請求項 4 3】

請求項 4 2 に記載の通信システムにおいて、

前記認証装置では、前記ドアロック制御装置から受信した前記識別情報と、前記第 2 の記憶部に記憶されている前記本鍵情報としての識別情報とを比較し、その比較結果を認証結果とする

ことを特徴とする通信システム。

【請求項 4 4】

請求項 4 3 に記載の通信システムにおいて、

前記認証装置は、前記サーバ装置からの本鍵情報の抹消登録要求を受けたときに、前記第 2 の記憶部の前記本鍵情報として登録されている識別情報を抹消し、前記バックアップ鍵情報として登録されている識別情報を本鍵情報として扱う

ことを特徴とする通信システム。

【請求項 4 5】

請求項 4 2 に記載の通信システムにおいて、

前記認証装置は、前記ドアロック制御装置から受信した前記識別情報と、前記第 2 の記憶部に記憶されている前記本鍵情報および前記バックアップ鍵情報としての識別情報とを比較し、その比較結果を認証結果とすることを特徴とする通信システム。

【請求項 4 6】

請求項 4 に記載の通信システムにおいて、

前記制御装置の前記第 2 の記憶部には、前記電子鍵情報は、個人情報と関連して記憶され、前記電子鍵情報は、個人識別情報としても用いられることを特徴とする通信システム。

【請求項 4 7】

請求項 1 0 に記載の通信システムにおいて、

前記認証装置の前記第 2 の記憶部には、前記電子鍵情報は、個人情報と関連して記憶され、前記電子鍵情報は、個人識別情報としても用いられることを特徴とする通信システム。

【請求項 4 8】

請求項 1 8 に記載の制御装置において、

前記記憶部には、前記電子鍵情報は、個人情報と関連して記憶され、前記電子鍵情報は、個人識別情報としても用いられることを特徴とする制御装置。

【請求項 4 9】

請求項 2 4 に記載の認証装置において、

前記記憶部には、前記電子鍵情報は、個人情報と関連して記憶され、前記電子鍵情報は、個人識別情報としても用いられることを特徴とする認証装置。

【請求項 5 0】

請求項 3 3 に記載の通信システムにおいて、

前記サーバ装置の第 3 の記憶部には、前記識別情報は個人情報と関連して記憶されると共に、前記制御装置の第 2 の記憶部においても、前記電子鍵情報として

の前記識別情報は個人情報と関連して記憶され、前記電子鍵情報は、個人識別情報としても用いられることを特徴とする通信システム。

【請求項 5 1】

請求項 4 0 に記載の通信システムにおいて、

前記サーバ装置の第 3 の記憶部には、前記識別情報は個人情報と関連して記憶されると共に、前記認証装置の第 2 の記憶部においても、前記電子鍵情報としての前記識別情報は個人情報と関連して記憶され、前記電子鍵情報は、個人識別情報としても用いられることを特徴とする通信システム。

【請求項 5 2】

請求項 1 8 に記載の制御装置において、

前記電子鍵情報を管理するサーバ装置と通信する通信手段を備え、

前記登録手段は、前記通信手段を通じて取得した前記識別情報を前記電子鍵情報として前記記憶部に記憶することを特徴とする制御装置。

【請求項 5 3】

請求項 2 4 に記載の認証装置において、

前記電子鍵情報を管理するサーバ装置と通信する通信手段を備え、

前記登録手段は、前記通信手段を通じて取得した前記識別情報を前記電子鍵情報として前記記憶部に記憶することを特徴とする認証装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

この発明は、電子鍵情報を用いてドアの施錠、開錠を制御するようにするドアロックシステムに用いて好適な通信装置および通信システムに関する。

【0002】

【従来の技術】

従来の物理的な鍵を鍵シリンダーに差し込んで施錠、開錠を行なうドアロックシステムにおいては、鍵を紛失した場合には、ドアロック機構の鍵シリンダーを当該鍵以外の鍵を用いるものに交換しない限り、悪意の紛失鍵の拾得者にドアが開錠されてしまうおそれがつきまとう。また、最近では、鍵シリンダー機構に精通

しているものが、鍵を用いずに開錠することによる盗難等の事件が発生している。

【0003】

そこで、このような鍵シリンダー機構を用いない電子鍵によるドアロックシステムが注目されている。例えば、この電子鍵によるドアロックシステムの一例として、親機は、予め登録されているIDコードと、電子鍵としての子機から受信したIDコードを比較照合して、その比較結果に基づいてドアロックをコントロールするものが知られている（例えば特許文献1参照）。

【0004】

【特許文献1】

特開平9-4293号公報。

【0005】

【発明が解決しようとする課題】

ところで、鍵を用いるシステムにおいては、鍵の紛失を考慮していわゆるスペア鍵を用意することが一般的に行なわれる。これは、電子鍵においても同様であり、通常は、鍵を複製してスペア鍵を作る。したがって、複数の同一鍵が用意されることになる。

【0006】

しかし、同一の鍵が複数になることは、それだけ鍵の紛失の機会も増えることになり、セキュリティ上、好ましくない。また、IDコードなどの識別情報を電子鍵情報として用いる場合に、たまたま同じIDコードが異なる電子鍵に登録されてしまうと、同様に、セキュリティ上、好ましくない。

【0007】

この発明は、以上の問題点を解決することができる通信装置および通信システムを提供することを目的とする。

【0008】

【課題を解決するための手段】

上記課題を解決するために、請求項1の発明による通信装置は、同一のものが存在しないように一元管理されて割り振られた識別情報を記憶す

る記憶部と、

ドアの施錠、開錠を行なうためのドアロック機構を制御するための制御装置との通信を行なう通信部と、

前記通信部を介して、前記記憶部の前記識別情報を、前記ドアの施錠、開錠を制御するための電子鍵情報として、前記制御装置に送信するように制御する制御部と、

を備えることを特徴とする。

【0009】

この請求項1の発明によれば、電子鍵として使用される識別情報は、同一のものが存在しないように一元管理されており、各通信装置には、異なる識別情報が記憶されることになる。したがって、この識別情報が電子鍵情報として用いられれば、セキュリティ上、好ましい。

【0010】

請求項4の発明による通信システムは、

電子鍵情報に応じてドアの施錠、開錠を行なうためのドアロック機構を制御する制御装置と、前記制御装置に前記電子鍵情報を送信する通信装置とからなる通信システムであって、

前記通信装置は、

同一のものが存在しないように一元管理されて割り振られた識別情報を記憶する第1の記憶部と、

前記制御装置との通信を行なうための第1の通信部と、

前記第1の通信部を介して、前記第1の記憶部の前記識別情報を、前記ドアの施錠、開錠を制御するための電子鍵情報として、前記制御装置に送信するように制御する第1の制御部と、

を備え

前記制御装置は、

前記通信装置と通信を行なうための第2の通信部と、

前記電子鍵情報としての前記識別情報を記憶する第2の記憶部と、

前記第2の記憶部に前記識別情報を前記電子鍵情報として登録するための登録

手段と、

前記第 2 の通信部を通じて前記通信装置から受信した前記識別情報と、前記第 2 の記憶部に記憶されている識別情報とを比較し、その比較結果に基づいて前記ドアの施錠、開錠を制御する第 2 の制御部と、

を備えることを特徴とする。

【0011】

この請求項 4 の通信システムにおいては、ドアの施錠、開錠を制御する制御装置の第 2 の記憶部には、同一のものが存在しないように一元管理されて割り振られた識別情報が電子鍵情報として記憶されている。そして、制御装置の第 2 の制御部は、通信装置から受信した識別情報と、第 2 の記憶部に記憶されている識別情報とを比較し、その比較結果に応じて、ドアの施錠、開錠を制御する。

【0012】

したがって、この請求項 4 の通信システムによれば、同一の電子鍵情報が複数個存在することはないから、セキュリティ上、非常に好ましい。そして、スペア鍵が必要とされる場合には、請求項 5 の通信システムのように、制御装置の第 2 の記憶部に、複数の電子鍵情報を登録しておけばよい。

【0013】

【発明の実施の形態】

以下、この発明による通信装置および通信システムの実施形態を、図を参照しながら説明する。

【0014】

以下に説明する例では、家の玄関ドアには通信装置の例としての電子鍵装置からの電子鍵情報を受信してドアの施錠、開錠を制御するドアロック制御システムを設け、また、家の中には、窓や玄関ドアからの賊の侵入、火災の発生、ガス漏れを検知して、それぞれの異常事態に対応する措置を取るセキュリティ監視システムを設け、このセキュリティ監視システムとドアロック制御システムとを、通信可能に接続して連動させて動作させるようにしている。そして、さらに、この例では、セキュリティ監視システムは、通信ネットワークを通じて管理サーバに接続して、全体として、実施形態の通信システムを構成している。

【0015】

そして、電子鍵装置としては、種々の形態のものを使用可能であるが、この例では、制御用 IC (Integrated Circuit) と、通信手段とが埋め込まれた装置が用いられる。そして、この例では、この電子鍵装置の具体例としては、ICカード（以下、電子鍵装置という）の他、携帯電話端末、PDA (Personal Digital Assistants) 端末などが用いられる。

【0016】

すなわち、この例では、電子鍵装置として、電子鍵装置のみでなく、携帯電話端末やPDA端末なども使用可能とされる。通常は、本鍵装置としてICカードが用いられ、携帯電話端末やPDA端末などはバックアップ端末（スベア）として用いられるようにされる。

【0017】

この場合に、この実施形態では、各電子鍵装置に搭載される制御用 IC はメモリを備え、そのメモリには、同一のものが存在しないように一元管理された識別情報が記憶される。この例では、この識別情報としては、ICチップ製造番号が用いられる。

【0018】

例えば、図1に示すように、1社あるいは複数社のICチップの製造会社1001において、製造した制御用ICチップ1002に対して、一元管理された重複のないICチップ製造番号を付与するようにする。ICチップの製造会社1001が複数社の場合には、例えば、それぞれのICチップ製造会社1001に、予め、制御用ICチップ1002に付与する製造番号を割り当てておくようにすることにより、一元管理される。したがって、製造された制御用ICチップ1002のメモリには、互いに異なるICチップ製造番号が識別情報として記憶される。

【0019】

この制御用ICチップ1002は、ICカード製造工場（あるいは製造会社）1003、携帯電話端末製造工場（あるいは製造会社）1004、PDA端末製

造工場（あるいは製造会社）1005などに供給されて、それらの制御用ICチップと通信手段とが搭載されたICカード、携帯電話端末、PDA端末などが製造される。

【0020】

図2は、この実施形態で用いられるICチップ製造番号の一例を説明するための図である。

【0021】

この例のICチップ製造番号は、3桁のメーカー番号と、3桁のカテゴリコードと、4桁のシリアル番号とからなる、合計10桁の番号（記号を含む）で構成される。

【0022】

なお、識別情報は、ICチップ製造番号の限定されるものではなく、同一のものが存在しないように一元管理された情報であれば、どのようなものも使用可能である。また、識別情報は、ICチップ製造番号と共に、別個にICのメモリに記憶するようにしてもよい。

【0023】

電子鍵装置の通信手段としては、電磁誘導や電波を用いた非接触による通信手段が用いられる。この実施形態においては、この通信手段は、例えば数ミリメートル～数十センチメートルの範囲で通信ができるものであればよく、小パワーのもので十分である。

【0024】

次に、この実施形態の通信システムに用いられるドアロック制御システムにおいては、玄関ドアには、電子鍵装置によりドアの施錠、開錠を行なえるようにするためのドアロック装置が取り付けられる。この例では、電子鍵装置とドアロック装置との間では、鍵情報の通信を行ない、ドアロック装置は、その通信に基づいてドアの施錠、開錠を制御するようにする。

【0025】

この例では、電子鍵装置とドアロック装置との間の通信は、以下に説明する例では、電磁誘導を用いた非接触による通信とされており、後述するように、ドア

ロック装置の一部を構成する電子鍵装置のリード／ライト部を介して、通信が行われる。

【0026】

ドアの施錠、開錠を制御するための鍵情報としては、前述したＩＣチップ製造番号からなる識別情報が用いられる。当該家に住む住人（この明細書の説明では、簡単のため、家族構成員とする）の全員に共通の一つとして、各人が、その共通鍵情報を格納する電子鍵装置をそれぞれ持つようにすることもできるが、それでは、前述したような不具合が生じるおそれがある。

【0027】

そこで、この実施形態では、当該家における電子鍵情報として、前述のようにして一元管理された識別情報が内蔵メモリに書き込まれた電子鍵装置の前記識別情報を電子鍵情報として管理サーバ装置に登録することにより、家族構成員のそれぞれが、自分用の電子鍵装置を所有して使用するようになる。

【0028】

管理サーバ装置は、登録された家族構成員のそれぞれについての電子鍵情報をドアロック装置の電子鍵情報の記憶部に転送して、電子鍵情報をドアロック装置に登録させるようにする。ドアロック装置は、登録された電子鍵情報と、通信装置としての電子鍵装置から受信した電子鍵情報とを比較し認証して、その結果に応じてドアの施錠、開錠を制御する。

【0029】

後述するように、この実施形態では、家族構成員のそれぞれは、自分用の電子鍵情報として、本鍵情報と、バックアップ鍵情報とを管理サーバ装置に登録することができる。電子鍵情報は、前述したように、電子鍵装置ごとに異なるので、本鍵情報とバックアップ鍵情報との登録は、本鍵装置と、バックアップ鍵装置との登録に等しい。

【0030】

この実施形態では、本鍵装置としては、ドアロック制御システムの提供会社が提供するＩＣカードとされる。そして、この本鍵装置であるＩＣカードの識別情報が、ドアロック制御システムが当該家に取り付けられる前に、予め管理サーバ

装置に電子鍵情報として登録される。

【0031】

この場合に、この実施形態では、家族構成員の数分だけ、ＩＣカードが前記提供会社から提供され、それらの複数のＩＣカードの全ての識別情報が、設置されるドアロック制御システム用の電子鍵情報として管理サーバ装置に登録される。

【0032】

さらに、この実施形態では、管理サーバ装置には、ドアロック制御システムが設置される家の家族構成員のそれぞれについての個人情報が収集され、その個人情報に対応して、それぞれの家族構成員が持つＩＣカードの識別情報が登録される。したがって、ドアロック制御システムは、電子鍵情報を検索することにより、それが誰の電子鍵情報であるかを判別することができる。つまり、この例の通信システムにおいては、電子鍵情報を、家族構成員の個人識別情報として用いることが可能である。

【0033】

そして、管理サーバ装置に登録された各家族構成員の本鍵情報は、ドアロック制御システムが、当該家に設置された後、システムの設置事業者や、ユーザが管理サーバ装置に対して初期登録要求をすることにより、ドアロック装置の記憶部に登録され、電子鍵情報の認証用として使用されることになる。

【0034】

また、この実施形態では、本鍵装置を紛失してしまった場合を考慮して、バックアップ鍵情報を登録しておくことができる。後述するように、この実施形態では、バックアップ鍵情報は、家族構成員の各人が、バックアップ鍵装置として使用したい電子鍵装置の識別情報（この例では、ＩＣ製造番号）を管理サーバ装置に登録することにより、登録可能である。

【0035】

なお、本鍵情報とバックアップ鍵情報との電子鍵情報の認証についての取り扱い方法としては、本鍵情報とバックアップ鍵情報とを同等に扱う方法と、認証用としては本鍵情報のみを原則とし、本鍵情報が抹消されたときに、バックアップ鍵情報が登録されていれば、以後は、バックアップ鍵情報を本鍵情報として取り

扱うようにする方法とがある。いずれの方法を用いることができるが、できるだけ、認証用としては、少ない方がセキュリティ上は好ましいと考えられるので、この実施形態では、後者の場合を採用するものとしている。

【0036】

前述したように、この実施形態においては、電子鍵情報として用いる識別情報は、個人識別情報としても用いることができることを利用して、各家族構成員個々の玄関ドアからの入退出を管理することができるようにする。

【0037】

このように電子鍵情報を個人識別情報としても用いることにより、当該家に住む家族構成員それぞれの玄関ドアからの入退出の管理情報を、セキュリティシステムに反映させることができ、より高機能のセキュリティシステムを構築することができる。

【0038】

[実施形態のドアロックシステムを含むセキュリティシステムの概要]

図3は、ドアロック制御システムおよびセキュリティシステムを含む、この実施形態の通信システムの概要を説明するための図である。

【0039】

家の玄関ドア1には、電子鍵装置と通信を行なうドアロック装置2が取り付けられている。室内には、セキュリティシステムを構成する監視制御装置3が設けられ、ドアロック装置2と接続されている。ドアロック装置2と監視制御装置3とは、この例では接続線により接続されるが、無線により接続するようにしてもよい。

【0040】

監視制御装置3は、ドアロック装置2からの電子鍵情報を受け取って、前述した電子鍵情報の認証を行なう装置、つまり認証装置となることもできる。しかし、この例では、電子鍵情報の認証は、ドアロック装置2自身において行なうようにされている。

【0041】

そして、この例では、室内には、火災発生を検知する火災センサ4と、ガス漏

れを検知するガスセンサ 5 と、窓の戸締りを検知する窓センサ 6 a, 6 b と、テレビ 7 が設けられ、それぞれ監視制御装置 3 に接続されている。監視制御装置 3 とそれらとの接続も、接続線により接続されているが、無線により接続してもよい。

【0042】

また、図 3 では省略したが、火災センサ 4 で火災発生を検知したときに、その発生現場近傍を撮影できるような位置や、窓センサ 6 a, 6 b で賊の侵入を検知したときに、その賊を撮影できるような位置には、監視カメラを設けるようにすることができる。その場合には、それら監視カメラは監視制御装置 3 に接続され、監視カメラの撮影画像が監視制御装置 3 に供給されるようにされる。

【0043】

監視制御装置 3 は、また、電話回線 8 を通じ、通信ネットワーク 9 を通じてセキュリティシステムの管理会社が運営する管理サーバ装置 10 に接続される。この管理サーバ装置 10 も、ドアロック装置 2 からの電子鍵情報を、監視制御装置 3 を介して受け取ることにより、電子鍵情報の認証を行なう装置となることもできる。

【0044】

通信ネットワーク 9 は、携帯電話網をも含み、後述するように、監視制御装置 3 は、異常状態の発生時に、予め登録された携帯電話端末 11 a, 11 b に、当該異常状態の発生を知らせることが可能とされている。さらに、通信ネットワーク 9 は、インターネットを含み、パーソナルコンピュータ 12 は、管理サーバ装置 10 に対して当該インターネットを通じてアクセスすることが可能とされている。また、携帯電話端末 11 a, 11 b から、管理サーバ装置 10 にアクセスすることが可能とされている。

【0045】

次に、ドアロック装置 2 の具体的構成例およびその動作、また、監視制御装置 3 の具体的構成例およびその動作について、詳細に説明する。なお、以下に説明する例では、前述したように、電子鍵情報の認証は、ドアロック装置自身が行なうものとする。

【0046】

[ドアロック装置の構成]

図4 (A) および図4 (B) は、ドアロック装置2の構成例を説明するための図である。図4 (A) は、家の外側から玄関ドア1のドアロック装置2の取り付け部分近傍を見た図である。また、図4 (B) は、玄関ドア1のドアロック装置2の取り付け部分近傍を、玄関ドア1の端面側から見た図である。

【0047】

この例のドアロック装置2においては、玄関ドア1の外側（戸外側）には、電子鍵装置と通信を行なうための外側電子鍵リーダ／ライタ部21exと、電子鍵情報の認証結果や玄関ドア1の施錠または開錠を視覚的に知らせるための表示素子の例としての外側LED (Light Emitting Diode; 発光ダイオード) 22exと、電子鍵情報の認証結果や玄関ドア1の施錠または開錠を音声により知らせるための外側スピーカ23exと、外側ドアノブ24exとが設けられている。

【0048】

また、玄関ドア1の内側（屋内側）にも、電子鍵装置と通信を行なうための内側電子鍵リーダ／ライタ部21inと、電子鍵情報の認証結果や玄関ドア1の施錠または開錠を視覚的に知らせるための表示素子の例としての内側LED 22inと、電子鍵情報の認証結果や玄関ドア1の施錠または開錠を音声により知らせるための内側スピーカ23inと、内側ドアノブ24inとが設けられている。

【0049】

玄関ドア1には、さらに、玄関ドア係止片25と、ロック片26と、ドア開閉センサ27が設けられている。さらに、玄関ドア1の内側には、ドアロック装置2の動作を制御するためのドアロック制御装置100が設けられており、電子鍵リーダ／ライタ部21exおよび21in、LED 22exおよび22in、スピーカ23exおよび23in、ドア開閉センサ27および図示を省略したドアロック機構駆動部が、このドアロック制御装置100に接続されている。

【0050】

玄関ドア係止片25は、ドアノブ24exあるいはドアノブ24inの操作に

応じて、玄関ドアの端面 1 a に垂直な方向に摺動移動する部材である。これは、後述するオートロックモードでない場合において、玄関ドア 1 が施錠されていないときにも、玄関ドア 1 の端面 1 a と対向する壁の端面側に設けられる凹部に勘合して、玄関ドア 1 を、係止するためのものである。

【0051】

ロック片 26 は、ドアロック機構の一部を構成する部材であり、図 4 では図示を省略したドアロック機構駆動部によりドアロック機構が駆動されることにより、玄関ドアの端面 1 a に垂直な方向に摺動移動して、玄関ドア 1 を施錠するときには、図 4 のように、玄関ドア 1 の端面 1 a から突出する状態に固定され、玄関ドア 1 を開錠するときには、玄関ドア 1 の端面 1 a から突出しない状態に固定される。

【0052】

なお、図示は省略したが、玄関ドア 1 の端面 1 a と対向する壁の端面には、このロック片 26 が突出した状態のときに嵌合される凹部が形成されており、ロック片 26 が当該凹部に嵌合される状態が玄関ドアの施錠状態となる。そして、ロック片 26 が玄関ドア 1 側に引っ込んで、当該凹部に嵌合していないときには、施錠状態が解除されて、開錠状態になる。

【0053】

玄関ドア開閉センサ 27 は、例えば光学式センサが用いられ、玄関ドア 1 が開けられたときは外部光を検知することにより、それを検知し、玄関ドア 1 が閉じられたときには、玄関ドア 1 の端面 1 a が、壁の端面と衝合することにより外部光が遮断されることを検知することにより、それを検知して、玄関ドア 1 の開閉を検知する。

【0054】

[ドアロック制御装置 100 の説明]

次に、ドアロック制御装置 100 を中心にしたドアロック装置 2 の電氣的な構成例を図 5 に示す。

【0055】

すなわち、ドアロック制御装置 100 は、マイクロコンピュータの構成を備え

ており、CPU (Central Processing Unit) 101 に対してシステムバス 102 を介してプログラムやデータが記録されている ROM (Read Only Memory) 103 と、ワークエリア用 RAM (Random Access Memory) 104 と、家族構成員の個々についての電子鍵情報となる識別情報 (この例では、IC 製造番号) が記憶されている家族情報メモリ 120 と、監視制御装置 3 と通信を行なうための通信インターフェース 121 とが接続されている。

【0056】

家族情報メモリ 120 には、後述するように、管理サーバ装置 10 に登録された本鍵情報やバックアップ鍵情報が、家族構成員のそれぞれについて、電子鍵情報として登録されて格納されている。また、各家族構成員を識別するための情報、例えば、氏名、年齢、性別、続き柄、その他の個人情報も、併せて家族情報メモリ 120 に格納するようにしてもよい。この家族情報メモリ 120 への電子鍵情報の登録に関しては、後述する。

【0057】

また、システムバス 102 には、インターフェース 105 および 106 を介して内側電子鍵リード／ライト部 21in および外側電子鍵リード／ライト部 21ex が接続され、また、内側 LED 駆動部 107 を介して内側 LED 22in が接続され、外側 LED 駆動部 108 を介して外側 LED 22ex が接続され、さらに、音声出力インターフェース 109 を介して内側スピーカ 23in が接続され、音声インターフェース 110 を介して外側スピーカ 23ex が接続される。

【0058】

さらに、システムバス 102 には、インターフェース 111 を介してドア開閉センサ 27 が接続されると共に、ドアロック機構駆動部 112 を介して、ロック片 26 を摺動駆動させるドアロック機構 28 が接続される。

【0059】

電子鍵リード／ライト部 21ex または 21in は、電子鍵装置 40 と通信を行なう通信部を構成する。電子鍵リード／ライト部 21ex または 21in は、この例では、電磁誘導アンテナおよび情報送受信部を含む。

【0060】

この例のドアロック制御装置100は、ドアロック制御モードとして、オートロックモードと、逐次ロックモードとの2通りの制御モードを備えている。

【0061】

オートロックモードは、ドアロック制御装置100が、電子鍵リード／ライト部21ex, 21inを介して電子鍵装置40と通信することに基づき玄関ドア1を開錠した後、所定時間後に自動的に玄関ドアを施錠状態にするモードである。オートロックモードにおいては、常に、内側と外側の電子鍵リード／ライト部21ex, 21inの両方を用いるものとなる。

【0062】

また、逐次ロックモードは、少なくとも玄関ドア1の外側の電子鍵リード／ライト部21exを通じて電子鍵装置40と通信することに基づき玄関ドアの施錠、開錠の状態を、そのときの状態とは逆の状態にするモードである。この逐次ロックモードにおいても、内側と外側の電子鍵リード／ライト部21ex, 21inの両方を用いることができるが、内側は、別途のマニュアルの施錠手段により施錠するようにした場合には、外側の電子鍵リード／ライト部21exを通じた電子鍵装置40との通信のみにより、玄関ドアの施錠、開錠動作を行なわせるようにすることができる。この逐次ロックモードは、従来からの一般的な鍵による施錠、開錠の方法に合わせたモードである。

【0063】

ドアロック装置2のドアロック制御モードをオートロックモードとするか、逐次ロックモードとするかの選択設定は、この例では、例えば、ドアロック装置2を取り付ける際に、後述するように、作業者により監視制御装置3を通じて行なわれる。

【0064】

ドアロック装置2がいずれのドアロック制御モードに設定されているかの情報は、ドアロック制御装置100内の図示を省略した不揮発性メモリに格納されており、ドアロック制御装置100は、当該不揮発性メモリの記憶情報を参照することにより、自装置のドアロック制御モードが、オートロックモードか、逐次ロ

ックモードかを認識するものである。監視制御装置 3 を通じたドアロック制御モードの設定動作に関しては、後述する。

【0065】

なお、ドアロック装置 2 のドアロック制御モードをオートロックモードとするか、逐次ロックモードとするかの選択設定は、監視制御装置 3 を通じて行なうのではなく、ドアロック装置 2 に直接的に行なうようにすることもできる。例えば、予め、ドアロック装置 2 の出荷時に、いずれのドアロック制御モードにするかの設定をドアロック装置 2 に行なっておくようにしても良い。また、ドアロック装置 2 に、ドアロック装置 2 の設置作業者が操作可能な入力操作手段、例えばディスプレイスイッチ等を設けておき、当該入力操作手段を通じて、ドアロック制御モードの設定を行なうようにしてもよい。

【0066】

[電子鍵装置 40 の構成例]

前述したように、この実施形態においては、電子鍵装置 40 としては、IC カードの他、携帯電話端末や PDA 端末なども用いることができる。しかし、電子鍵装置 40 は、電子鍵情報用の制御用 IC チップと通信手段とを備える点では共通している。

【0067】

図 6 は、電子鍵装置 40 が IC カード 40C である場合の構成例を示す図である。図 6 (A) は、IC カード 40C の表面を示し、この表面には、所有者の氏名と、ID 番号が表示されている。また、図 6 (B) は、IC カード 40C の内部構成例を示しており、IC カード 40C 内には、電子鍵リード／ライト部と通信を行なうための電磁誘導用のアンテナ 41 と、制御用 IC 42 とが内蔵されている。

【0068】

制御用 IC 42 内には、メモリを含み、前述した IC 製造番号からなる識別情報、所有者の氏名、住所の他、所有者のその他の必要な個人情報が記憶されている。この個人情報は、父親、母親、子供などの区別が可能ないように構成されている。また、制御用 IC 42 内のメモリに、各所有者が行った電子鍵リード／ライ

ト部 21ex または 21in との通信の時刻や履歴（内側と外側のどちらの電子鍵リード／ライト部と通信したか情報を含む）や、各所有者の外出、帰宅の履歴などを書き込むようにされている。

【0069】

なお、これらの履歴情報は、ドアロック制御装置 100 の家族情報メモリ 120 や監視制御装置 3 の後述の家族情報メモリ 205 における各人に対応するエリアにも記憶されるものである。

【0070】

図 7 は、IC カード 40C の内部ブロック構成を示すものである。CPU 401 に対してシステムバス 402 を介してプログラムやデータが記録されている ROM 403 と、ワークエリア用 RAM 404 と、電子鍵情報となる識別情報（この例では、IC 製造番号）が記憶されている識別情報メモリ 405 と、通信履歴メモリ 406 と、送受信インターフェース 407 とが接続されている。識別情報メモリ 405 には、使用者の個人情報をも記憶することが可能である。

【0071】

送受信インターフェース 407 には、電磁誘導アンテナ 41 に接続されている情報送受信回路 408 が接続されている。そして、識別情報メモリ 405 から読み出した識別情報を送受信インターフェース 407、情報送受信回路 408 および電磁誘導アンテナ 41 を通じて送出する。

【0072】

また、電磁誘導アンテナ 41 にて受信した情報を、情報送受信回路 408 および送受信インターフェース 407 を通じて取り込み、通信履歴メモリに書き込んだりする。

【0073】

[監視制御装置 3 の外観の説明]

図 8 は、室内に設けられるセキュリティシステム用の監視制御装置 3 の構成を説明するための外観図であり、この監視制御装置 3 は、例えば赤外線や電波を用いたリモートコマンド 50 によりリモコン制御可能の構成とされている。

【0074】

監視制御装置 3 の筐体 30 には、ビデオカメラ 31 が組み込まれている。このビデオカメラ 31 は、この例では、実線位置の横置き状態と、点線位置の縦置き状態とのいずれの状態をも取れる機構により、筐体 30 に対して取り付けられている。このビデオカメラ 31 は、セキュリティモードがオンとされたときに、監視制御装置 3 からの指示により撮影を開始するようにされている。

【0075】

また、ビデオカメラ 31 による撮影方向は、ビデオカメラが首振り方向に調整可能な構造とされているので、その調整により変えられるようにされている。したがって、使用者は、セキュリティモードオンに先立ち、ビデオカメラ 31 による撮影方向の調整を行なっておくことができる。

【0076】

そして、筐体 30 には、ビデオカメラ 31 による撮影対象部を明るく照明するための撮影用ランプ 32 が設けられている。また、筐体 30 には、例えば遠赤外線を検知することにより人を検知する人感センサ 33 が設けられている。監視制御装置 3 は、後述するように、セキュリティモードオンのときに人感センサ 33 で人を検知したときには、賊の侵入であるとして検知し、撮影用ランプ 32 をオンにすると共に、所定の通報先に撮影画像を送るようにする。

【0077】

筐体 30 には、また、マイクロホン 34 とスピーカ 35 とが設けられている。マイクロホン 34 は、賊の声や賊侵入時の室内の臨場音を收音するためのものである。スピーカ 35 は、侵入してきた賊を威嚇する音声を放音するためなどに用いられる。

【0078】

筐体 30 には、また、電子鍵リード／ライト部 36 が設けられる。この電子鍵リード／ライト部 36 は、この例では、伝言の記録、再生の際に用いられる。すなわち、この例においては、監視制御装置 3 は、伝言装置の役割もできるように構成されており、電子鍵リード／ライト部 36 により、電子鍵装置を読み取らせした後、後述するようにリモートコマンド 50 の伝言記録ボタンを押すと、設定した相手（家族の誰か）に伝言が残すことができ、また、リモートコマンド 50 の

伝言再生ボタンを押すと、自分宛ての伝言を再生することができるようになって
いる。

【0079】

この伝言が記録されているかどうかなどを知らせるため等の用途として、筐体
30には、複数のLED37が設けられている。また、筐体30には、さらに
、リモートコマンド50からのリモコン信号の受信部38が設けられる。

【0080】

また、図5では図示を省略したが、監視制御装置3の背面パネルには、テレビ
受像機7のビデオ入力端子に接続される映像出力端子が設けられている。そして
、監視制御装置3には、テレビ受像機7の電源のオン・オフなどを制御するため
のリモコン送信部39が設けられている。

【0081】

さらに、監視制御装置3は、火災センサ4、ガスセンサ5、窓センサ6a, 6
b、さらには、監視カメラを接続するためのセンサハブを備えている。また、図
3で説明したように、監視制御装置3は、電話回線を通じて、セキュリティシス
テムの管理会社が運営する管理サーバ装置10にアクセスできるように構成され
ている。

【0082】

[監視制御装置3の構成例]

監視制御装置3の内部構成および監視制御装置3と周辺機器との接続状態の構
成例を図9に示す。

【0083】

監視制御装置3は、マイクロコンピュータの構成を備えており、CPU201
に対して、システムバス202を介して、プログラムやデータが記録されている
ROM (Read Only Memory) 203と、ワークエリア用RAM
(Random Access Memory) 204と、ドアロック制御装置
100の家族情報メモリ120と同様に、電子鍵装置40を所有する家族全員の
電子鍵情報となる識別情報が記憶されている家族情報メモリ205と、ドアロッ
ク制御装置100と通信を行なうためのドアロック装置通信インターフェース2

06と、センサハブ207と、ビデオカメラ31の撮影画像およびマイクロホン34で収音した音声を記憶するための画像・音声メモリ208と、電話回線を通じて管理サーバ装置10等と通信を行なうための通信インターフェース209とが接続されている。

【0084】

また、システムバス202には、カメラインターフェース210を介してビデオカメラ31が、インターフェース211を介して撮影用ランプ32の照明機構320が、インターフェース212を介して人感センサ33が、インターフェース214を介して電子鍵リード／ライト部36が、インターフェース215を介してリモコン受信部38が、インターフェース216を介してリモコン送信部39が、音声入力インターフェース218を介してマイクロホン34が、インターフェース219を介してLED37が、音声出力インターフェース220を介してスピーカ35が、それぞれ接続されている。さらに、システムバス202は、ビデオ信号出力端子からなるテレビインターフェース217を介してテレビ受像機7に接続されている。

【0085】

家族情報メモリ205は、例えばEEPROM (Electrically Erasable Programmable ROM) で構成される。

【0086】

家族情報メモリ205には、ドアロック制御装置100の家族情報メモリ120と同様に、家族構成員のそれぞれについての識別情報と、個人情報とが格納されている。この明細書では、識別情報と個人情報とからなる情報を、個人プロフィール情報と呼ぶことにする。

【0087】

図10に、一人分の個人プロフィール情報の例を示す。図10に示すように、個人プロフィール情報は、個人識別情報と個人情報とが対応付けられて記憶された情報である。この実施形態では、個人識別情報は、前述したように、電子鍵装置の各メモリに格納されている識別情報が用いられる。個人識別情報は個人情報と対応させることで、具体的に誰の識別情報であるかが判明する。この識別情報

は、電子鍵情報の役割を有することは前述した通りであり、図10に示すように、電子鍵情報としては、本鍵情報とバックアップ鍵情報とが登録可能である。バックアップ鍵情報は、複数個、登録可能としてもよい。

【0088】

図10の例においては、個人情報としては、パスワード情報、氏名、住所、生年月日、年齢、続柄、登録日、銀行口座番号、電話番号、趣味／嗜好情報、家の玄関8からの入退出履歴情報、電子鍵登録・紛失履歴情報などが家族情報メモリ205に記憶される。

【0089】

この例の入退出履歴情報には、外出時刻、帰宅時刻が記憶されるほか、外出中であるか、在宅であるかの在／不在フラグが含まれる。この入退出履歴情報は、監視制御装置3が玄関ドア7を通じての家族の入退出を管理するために用いられる。また、電子鍵登録・紛失履歴情報は、後述するように、管理サーバ装置10からの電子鍵情報のバックアップ登録要求や抹消要求が到来して、バックアップ登録や抹消処理をしたときに、その日付、時刻とともに、バックアップ鍵情報や抹消した電子鍵情報を、バックアップ登録および抹消の区別をして記録しておくものである。

【0090】

さらに、この例では、この家族情報メモリ205には、セキュリティモード用の情報も格納されている。すなわち、この例では、監視制御装置3では、家族構成員の在宅状況に応じて、セキュリティレベルを変更することが可能なように構成されている。図11は、セキュリティレベルと家族構成員の在宅状況との関係を示すテーブルである。また、図12は、セキュリティレベルとセキュリティ内容との対応を示すテーブルである。

【0091】

図12に示すように、この例においては、セキュリティレベルは、セキュリティレベルが高い方から順に、レベルA、レベルB、レベルC、レベルDまであり、レベルAにおいては、窓および玄関ドアの監視、火災やガス漏れの監視、ビデオカメラ31による監視の全てを行ない、レベルBでは、ビデオカメラ31によ

る監視は行なわずに、窓および玄関ドアの監視および火災やガス漏れの監視を行ない、レベルCでは、火災やガス漏れの監視のみを行ない、レベルDでは、監視を行なわない、という内容である。

【0092】

そして、図11に示すように、家族構成員の在宅状況のそれぞれに対して各セキュリティレベルが割り付けられる。すなわち、この例では、父親が在宅の状況では、監視を行なわないレベルDとされる。また、父親が不在であるが母親が在宅の状況では、火災やガス漏れの監視のみを行なうレベルCとされる。また、子供のみが在宅の状況では、窓および玄関ドアの監視および火災やガス漏れの監視を行なうレベルBとされる。そして、全員が不在である状況では、全ての監視を行なうレベルAとされる。

【0093】

監視制御装置3では、セキュリティモードをオンにするとき、また、セキュリティレベルを変更するとき、これら図11、図12のテーブルを参照し、在宅状況に応じてセキュリティレベルを決定するようにする。

【0094】

図11のセキュリティレベルと、家族構成員の在宅状況との関係は、予め設定しておくこともできるし、使用者が、例えばリモートコマンド50を用いて監視制御装置3に入力設定することにより、設定を変更することできるように構成されている。

【0095】

なお、これら図11、図12のテーブル情報は、家族情報メモリ205ではなく、別のメモリに格納するようにしても良いことは言うまでもない。

【0096】

ドアロック装置通信インターフェース206は、ドアロック制御装置100に接続されている。センサハブ207には、火災センサ4、ガスセンサ5、窓センサ6a, 6bおよび1個あるいは複数個の監視カメラ13が接続される。

【0097】

画像・音声メモリ208は、セキュリティモードがオンであるときに、ビデオ

カメラ 31 で撮影した画像情報と、マイクロホン 34 で収音した音声情報とをバッファリングする監視情報領域と、伝言として記録されている画像情報および音声情報を記憶する伝言情報領域とを備えている。また、監視情報領域には、監視カメラ 13 用の画像記憶領域も設けられている。

【0098】

監視情報領域は、この例では、所定時間、例えば 30 秒分の画像情報および音声情報を、いわゆるリングバッファ形式で記憶する。なお、監視情報領域と伝言情報領域とは、別々のメモリの構成とすることも勿論できる。

【0099】

通信インターフェース 209 は、この例では、ルータ 61 に接続されている。ルータ 61 は、ADSL モデム 62、スプリッタ 63 を通じて電話回線 65 に接続されている。スプリッタ 63 には、電話端末 64 が接続される。

【0100】

[リモートコマンド 50 の説明]

監視制御装置 3 用のリモートコマンド 50 は、図 8 に示すように、セキュリティボタン 51 と、オフボタン 52 と、伝言記録ボタン 53 と、伝言再生ボタン 54 と、メニューボタン 55 と、上下左右の選択を行なう 4 個のキーとその中央の決定キーとからなるカーソルボタン 56 とを備えて構成されている。

【0101】

メニュー項目としては、この例では、管理サーバ装置 10 に対する電子鍵情報としての個人 ID の登録、ドアロック装置 2 のドアロック制御モードの設定、その他が、用意されており、それぞれのメニュー項目に対応する処理を実行するアプリケーションプログラムは、監視制御装置 3 の ROM 203 に格納されている。

【0102】

[管理サーバ装置 10 の構成]

次に、管理サーバ装置 10 の構成例を図 13 に示す。管理サーバ装置 10 は、コンピュータの構成を備えており、CPU 301 に対して、システムバス 302 を介して、プログラムやデータが記録されている ROM 303 と、ワークエリア

用RAM304と、ドアロック装置管理データベース305と、電子鍵登録・紛失履歴メモリ306と、インターネットなどの通信ネットワークを通じて通信を行なうための通信インターフェース307とが接続されている。また、システムバス302には、さらに、ホームページ用メモリ308と、画像・音声メモリ309とが接続されている。

【0103】

ドアロック装置管理データベース305には、ドアロック装置2のシリアル番号、ドアロック装置2が設置された住所、電話番号、ドアロック装置の利用者の氏名、登録された電子鍵情報など、ドアロック装置2の管理に必要な事項が格納されている。

【0104】

電子鍵登録・紛失履歴メモリ306には、各ドアロック装置2ごとに、電子鍵情報の登録と紛失の履歴が記憶される。ホームページ用メモリ308には、ホームページの各ページの表示情報が格納されており、CPU301の指示に従い、必要がページの表示情報が、このメモリ308から読み出されて、通信インターフェース307を通じて通信ネットワークに送出される。

【0105】

画像・音声メモリ309は、後述するように、セキュリティ監視システムから送られてくる画像・音声情報を格納する。管理サーバ装置10では、セキュリティ監視システムからの画像・音声をチェックして、警備会社に通知したり、ユーザの求めに応じて、画像・音声情報をホームページを通じて提供するようにする。

【0106】

次に、以上のような構成の通信システムにおける種々の動作について、以下に説明する。

【0107】

[監視制御装置3における伝言記録および伝言再生；図14]

前述したように、この例の監視制御装置3は、電子鍵装置40と、リモートコマンド50を用いて、特定の家人を指定して、伝言を記録しておくことができる

。伝言が監視制御装置 3 に記録されているときには、LED 37 が点灯あるいは点滅して、その旨を知らせるようにしている。

【0108】

そして、監視制御装置 3 に、伝言が記録されている場合には、帰宅した家人が、自分の電子鍵装置を、この電子鍵リード／ライト部 36 により読み取らせ、リモートコマンド 50 により伝言再生を指示すると、記録されている伝言が、その人宛ての伝言である場合には、監視制御装置 3 は、記録されている伝言を、テレビ受像機 7 やスピーカ 35 を通じて再生するようにするように構成されている。

【0109】

図 14 は、この伝言記録および再生のための監視制御装置 3 の処理を説明するためのフローチャートである。この図 14 の各ステップ S の処理は、CPU 201 が ROM 203 に記憶されているプログラムにしたがって実行されるものである。

【0110】

すなわち、まず、使用者は、伝言記録または伝言再生をするには、自分の電子鍵装置 40 を電子鍵リード／ライト部 36 にかざして、通信を行なうようにする。CPU 201 は、電子鍵リード／ライト部 36 で電子鍵装置 40 と通信が行われたか否か判別し（ステップ S1）、通信が行われたと判別すると、受信した識別情報により、誰の電子鍵装置 40 と通信したかを認識する（ステップ S2）。

【0111】

次に、リモートコマンド 50 からのリモコン信号の到来を待ち（ステップ S3）、リモコン信号を受信したことを確認したら、そのリモコン信号は、伝言記録ボタン 53 の操作によるものか否か判別し（ステップ S4）、伝言記録ボタン 53 の操作によるものであると判別したときには、CPU 201 は、伝言記録動作を行なうようにする（ステップ S12）。

【0112】

この伝言記録動作においては、監視制御装置 3 は、ビデオカメラ 31 で撮影された伝言者の画像情報をカメラインターフェース 210 を介して取り込み、画像

・音声メモリ 208 の伝言記録領域に格納すると共に、マイクロホン 34 で収音した伝言音声情報（伝言メッセージ）をインターフェース 218 を通じて取り込み、画像・音声メモリ 208 の伝言記録領域に格納する。このとき、それら画像情報および音声情報は、電子鍵装置 40 から読み込んだ識別情報に対応付けられて、当該識別情報と共に画像・音声メモリ 208 に格納される。

【0113】

次に、CPU 201 は、家族情報メモリ 208 に記憶されている家族の個人プロフィール情報を参照して、伝言記録をしようとしている操作者以外の伝言相手のリストをテレビ受像機 7 の画面に表示する（ステップ S14）。このとき、テレビ受像機 7 に電源が投入されていないときには、リモコン送信部 38 を通じて電源をオンにするリモコン信号をテレビ受像機 7 に供給して、テレビ受像機 7 に電源を投入しておく。なお、伝言相手のリストの画面は、例えばスーパーインポーズによりテレビ番組の画像に重ねて表示するようにしてもよいし、テレビ番組の画像に重ねることなく単独の画面としてもよい。

【0114】

操作者は、この伝言相手のリストから、リモートコマンド 50 のカーソルキー 56 を用いて、伝言相手の選択入力を行ない、カーソルキー 56 中の中央の決定キーを押す。監視制御装置 3 の CPU 201 は、この伝言相手の選択入力を受信して（ステップ S15）、当該伝言相手の情報を、画像・音声メモリ 208 の伝言記録領域の、前記画像情報および伝言音声メッセージに対応させて格納して登録する（ステップ S16）。そして、伝言が記録されたことを報知するために、1 個の LED 37 を点灯させる（ステップ S17）。LED 37 は、図 8 に示したように複数個設けられており、記録されている伝言の数だけ、点灯することとなる。

【0115】

また、ステップ S4 において、リモコン信号が伝言記録ボタン 53 の操作によるものではないと判別したときには、伝言再生ボタン 54 の操作によるものであるか否か判別する（ステップ S5）。伝言再生ボタン 54 の操作によるものではないと判別したときには、CPU 201 は、当該操作されたボタンに応じた処理を

行なう（ステップS6）。

【0116】

そして、ステップS5において、伝言再生ボタン54の操作によるものであると判別したときには、CPU21は、ステップS2で認識した識別情報を検索子として、画像・音声メモリ208の伝言記録領域の記憶内容を検索して、電子鍵装置40を電子鍵リード／ライト部36にかざした操作者宛ての伝言があるか否か判別する（ステップS7）。

【0117】

そして、ステップS7において、操作者宛ての伝言が無いと判別したときには、CPU201は、例えば予めROM203に用意されている「伝言はありません」の文字情報をテレビ受像機7の画面に表示すると共に、スピーカ35を通じて音声として放音して、操作者に報知する（ステップS8）。

【0118】

また、ステップS7において、操作者宛ての伝言があると判別したときには、当該操作者宛ての伝言画像および伝言音声を画像・音声メモリ208から読み出して、テレビ受像機7に表示すると共に、スピーカ35から放音して再生する（ステップS9）。

【0119】

伝言の再生が終了すると、CPU201は、テレビ受像機7の画面に伝言を消去するかどうかの問い合わせを表示するので、操作者は、その表示画面に含まれる「YES」、「NO」のいずれかをリモートコマンド50のカーソルキー56を用いて選択する。CPU201は、当該操作者の選択入力から、伝言を消去するか否か判別し（ステップS10）、消去すると判別したときには、画像・音声メモリ208の対応する画像・音声情報を消去し（ステップS11）、点灯しているLED37の一つを消灯する（ステップS12）。そして、この伝言記録再生処理ルーチンを終了する。

【0120】

また、ステップS10で、伝言を消去しないと判別したときには、そのまま、この伝言記録再生処理ルーチンを終了する。

【0121】

〔ドアロック制御モードの選択設定；図15、図16〕

前述したように、この実施形態では、監視制御装置3を通じてドアロック制御モードの設定ができるようにされているので、その設定動作を、図15のフローチャートを参照しながら説明する。

【0122】

先ず、監視制御装置3のCPU201は、リモコン受信部38の受信信号を監視して、ドアロック制御モードの設定を含む設定メニューのための特定のボタン操作がなされたか否か判別する（ステップS21）。この例では、この特定のボタン操作としては、通常の利用者が行なわない操作とされており、例えばセキュリティボタン51とメニューボタン55との同時操作などとされている。このような特定のボタン操作は、ドアロック装置2の設置業者等が設定作業を行なうために定義されている。簡単に、ドアロック制御モードの設定変更ができないようにするためである。

【0123】

ステップS21で、前記の特定のボタン操作はされないと判別されたときには、単独のボタン操作に応じた処理などの、その他の処理を行なう（ステップS22）。また、ステップS21で、前記の特定のボタン操作がされたと判別されたときには、設定メニューの一覧をテレビ受像機7の画面に、前述の伝言記録再生の場合と同様にして表示するようにする（ステップS23）。

【0124】

この設定メニューの一覧表示に対しては、操作者は、行ないたい設定メニュー項目の選択をリモートコマンド50のカーソルキーを用いて行なう。CPU201は、リモコン受信部38の受信信号を監視してメニュー項目の選択操作がなされたか否か判別し（ステップS24）、メニュー項目の選択操作がなされたと判別したときには、例えば反転表示して示す選択中項目を、選択操作に応じて変更する（ステップS25）。そして、設定項目の決定操作がなされたか否か判別する（ステップS26）。また、ステップS24で、メニュー項目の選択操作がされないと判別したときには、即座にステップS26に進んで設定項目の決定操

作がなされたか否か判別する。

【0125】

ステップS26で、設定項目の決定操作がなされないと判別したときには、ステップS24に戻る。また、ステップS26で、設定項目の決定操作がなされたと判別したときには、選択された設定項目はドアロック制御モードの設定であるか否か判別し（ステップS27）、そうではなかったときには選択された他の設定項目についての処理ルーチンを実行する（ステップS28）。

【0126】

ステップS27で、選択された設定項目はドアロック制御モードの設定であると判別したときには、CPU201は、テレビ受像機7の画面にオートロックモードと、逐次ロックモードとの選択画面を表示する（ステップS29）。操作者は、この選択画面において、いずれかの選択入力をカーソルキー56を用いて行なう。

【0127】

そこで、CPU201は、リモコン受信部38を監視して、オートロックモードが選択されたか否か判別し（ステップS30）、オートロックモードが選択されたと判別したときには、ドアロック装置2をオートロックモードに設定する設定動作を行なう（ステップS31）。

【0128】

すなわち、CPU201は、監視制御装置3に内蔵の不揮発性メモリ部のドアロック装置2のドアロック制御モードの記憶領域に、オートロックモードであることを示す情報を記憶すると共に、オートロックモードにする旨の指示をドアロック装置2に対して、ドアロック装置通信インターフェース206を通じて送る。

【0129】

また、ステップS30で、オートロックモードではないと判別したときには、CPU201は、逐次ロックモードが選択されたと判別して、ドアロック装置2を逐次ロックモードにする設定動作を行なう（ステップS32）。

【0130】

すなわち、CPU 201は、監視制御装置3に内蔵の不揮発性メモリ部のドアロック装置2のドアロック制御モードの記憶領域に、逐次ロックモードであることを示す情報を記憶すると共に、逐次ロックモードにする旨の指示をドアロック装置2に対して、ドアロック装置通信インターフェース206を通じて送る。

【0131】

以上で、監視制御装置3におけるロック制御モードの設定時の動作は終了となる。

【0132】

次に、ドアロック装置通信インターフェース206を通じて送られてきたドアロック制御モードの指示情報を受信したドアロック制御装置100の動作について、図11のフローチャートを参照して説明する。

【0133】

先ず、ドアロック制御装置100のCPU101は、ドアロック制御モードの設定指示情報を監視制御装置3から受け取ったか否か判別し（ステップS41）、受け取らないときには、その他の処理を行なう（ステップS42）。

【0134】

ステップS41で、ドアロック制御モードの設定指示情報を監視制御装置3から受け取ったと判別したときには、CPU101は、選択指示されたドアロック制御モードは、オートロックモードと逐次ロックモードのいずれであるか判別する（ステップS43）。

【0135】

ステップS43で、選択指示されたドアロック制御モードはオートロックモードであると判別したときには、CPU101は、ドアロック装置2のドアロック制御モードをオートロックモードに設定する処理を行なう（ステップS44）。

【0136】

すなわち、ステップS44においては、ドアロック制御装置100のCPU101は、オートロックモードの設定指示に基づき、ドアロック装置2の内側電子鍵リード／ライト部21inと、外側電子鍵リード／ライト部21exとの両方をアクティブにし、かつ、プログラムROM13のドアロック制御のアプリケー

ションを、オートロックモード用のものとするようにする。そして、CPU101は、ドアロック制御装置100が備える不揮発性メモリ部のドアロック制御モードの記憶領域に、オートロックモードであることを示す情報を記憶する。

【0137】

また、ステップS43で、選択指示されたドアロック制御モードは逐次ロックモードであると判別したときには、CPU101は、ドアロック装置2のドアロック制御モードを逐次ロックモードに設定する処理を行なう（ステップS45）。

。

【0138】

すなわち、ステップS45においては、ドアロック制御装置100のCPU101は、逐次ロックモードの設定指示に基づき、この例では、ドアロック装置2の内側電子鍵リード／ライト部21inと、外側電子鍵リード／ライト部21exとの両方をアクティブにし、かつ、プログラムROM13のドアロック制御のアプリケーションを、逐次ロックモード用のものとするようにする。そして、CPU101は、ドアロック制御装置100が備える不揮発性メモリ部のドアロック制御モードの記憶領域に、逐次ロックモードであることを示す情報を記憶する。

。

【0139】

なお、この例では、逐次ロックモードにおいても、内側電子鍵リード／ライト部21inと、外側電子鍵リード／ライト部21exとの両方を用いるようにしたが、この逐次ロックモードにおいては、外側電子鍵リード／ライト部exのみをアクティブにして、内側電子鍵リード／ライト部21inを用いないようにすることもできる。その場合には、家の内側からの施錠が問題になるが、例えば、内側からの玄関ドアの施錠を、電子鍵装置を用いずにマニュアル操作で行なえる構成とすればよい。

【0140】

次に、オートロックモードと、逐次ロックモードのそれぞれの場合のドアロック装置2の動作について説明する。以下に説明するフローチャートにおける各ステップSの動作は、ドアロック制御装置100のCPU101が主として実行す

る処理動作である。

【0141】

[オートロックモード；図17～図22]

オートロックモードのときの動作を、図17～図22のフローチャートを参照しながら説明する。このオートロックモードのときには、玄関ドア1は、定常状態では、施錠状態とされる。そして、電子鍵装置40が、内側電子鍵リード／ライト部21inまたは外側電子鍵リード／ライト部21exにかざされて通信が両者の間で行なわれ、識別情報、すなわち、電子鍵情報についての認証がとれたときには、所定時間のみ玄関ドアを開錠し、所定時間後に、自動的に玄関ドア1は施錠状態に戻るように、ドアロック制御装置100により制御されるものである。

【0142】

CPU101は、インターフェース105、106を介して、内側電子鍵リード／ライト部21inおよび外側電子鍵リード／ライト部21exを監視し、電子鍵装置40がかざされて、電子鍵装置40と内側電子鍵リード／ライト部21inまたは外側電子鍵リード／ライト部21exとの間で通信が行われるのを待つ（ステップS51）。

【0143】

そして、ステップS51において、電子鍵装置40がかざされて、電子鍵装置40と通信が行なわれたと判別したときには、CPU101は、識別情報を電子鍵装置40から受信し、例えばRAM104などに一時的に格納する（ステップS52）。このとき、ドアロック制御装置100が備える時計回路（図示を省略）の時刻情報が、電子鍵装置40に与えられ、制御用IC内42のメモリに書き込まれる。また、内側電子鍵リード／ライト部21inまたは外側電子鍵リード／ライト部21exのどちらと通信をしたかの情報として、通信相手のID等が制御用IC42のメモリに書き込まれる。

【0144】

次に、CPU101は、内側電子鍵リード／ライト部21inまたは外側電子鍵リード／ライト部21exのどちらで電子鍵装置40と通信が行われたかを判

別する（ステップS53）。その判別結果と、前記の通信の時刻情報とは、家族情報メモリ120の、前記識別情報に対応する家人の記録エリアにも書き込まれ、また、監視制御装置3にも、その家族情報メモリ205に記憶させるために転送される。

【0145】

[内側電子鍵リード／ライト部21inでの通信の場合；図17～図19]

ステップS53で、電子鍵装置40と通信が行われたのが内側電子鍵リード／ライト部21inであると判別したときには、CPU101は、在宅者が外出する場合であるとして、以下のような処理を行なう。なお、この例では、在宅者が玄関ドア1を開錠し、玄関ドア1を開けたときには、それまでにセキュリティモードがオンになっていても、一旦、セキュリティモードは、オフとされるものとしている。

【0146】

CPU101は、先ず、家族情報メモリ120に記憶されている識別情報と、電子鍵装置40から受信した識別情報とを比較して、家族情報メモリ120に記憶されている電子鍵情報としての識別情報の中に、電子鍵装置40から受信した識別情報と一致するものがあるかどうかにより、当該電子鍵装置40がドアロック装置2に登録された電子鍵装置であるか否かを判別して、当該電子鍵装置40についての認証を行なう（ステップS54）。

【0147】

そして、その認証結果を判別し（ステップS55）、家族情報メモリ120に記憶されている識別情報の中に、電子鍵装置40から受信した識別情報と一致するものがなくて、認証が取れなかったとき（認証NG）であると判別したときには、CPU101は、内側LED駆動部107を駆動して、内側LED22inを赤色で点滅させると共に、内側スピーカ23inから警告音を放音して、認証NGであることを電子鍵装置40の使用者に報知する（ステップS56）。そして、ドアロック機構28は施錠状態のままとして、ステップS51に戻る。

【0148】

また、ステップS55で、家族情報メモリ120に記憶されている識別情報の

中に、電子鍵装置 40 から受信した識別情報と一致するものがある、認証が OK であると判別したときには、CPU 101 は、内側 LED 駆動部 107 を駆動して、内側 LED 22 in を緑色で 1 秒間点灯させ、認証 OK であることを電子鍵装置 40 の使用者に報知する（ステップ S 57）。このとき、CPU 101 により、併せて内側スピーカ 23 in から「認証がとれました」というメッセージを放音させるようにしても良い。

【0149】

そして、このとき、認証が OK であることから、CPU 101 は、ドアロック機構駆動部 112 を駆動制御して、ドアロック機構 28 により玄関ドア 1 を開錠状態にし（ステップ S 58）、内側スピーカ 23 in から、「ドアロックを解除しました」というメッセージを放音させる（ステップ S 59）。このとき、内側 LED 22 in を、例えば緑色で点滅させ、ドアロックの解除状態を電子鍵装置 40 の使用者に報知するようにしてもよい。

【0150】

このとき、CPU 101 は、電子鍵装置 40 により内側から玄関ドア 1 が開錠されたことを認識していることに基づき、当該電子鍵装置 40 の使用者（在宅者）が外出しようとしていると認識する。そして、監視制御装置 3 に対して窓の開閉状態についての問い合わせを送る（図 13 のステップ S 61）。

【0151】

これに対して、監視制御装置 3 では、窓センサ 6 a, 6 b のセンサ出力をセンサハブ 207 を通じて取得して、窓の開閉を確認する。つまり、戸締りを確認する。そして、窓の開閉状態についての確認結果をドアロック装置インターフェース 206 を通じてドアロック制御装置 100 に返信するようにする。

【0152】

ドアロック制御装置 100 では、この窓の開閉状態についての確認結果を、通信インターフェース 121 を通じて受信する（ステップ S 62）。そして、CPU 101 は、受信した当該確認結果を解析して、窓が開放されているか否か判別する（ステップ S 63）。

【0153】

そして、窓が開いていると判別したときには、CPU101は、窓が開いていることを内側スピーカ23inからの放音音声により警告する（ステップS64）。また、窓が閉じていると判別したときには、CPU101は、戸締りがOKであることを内側スピーカ23inからの放音音声により報知する（ステップS65）。

【0154】

次に、CPU101は、ドア開閉センサ27のセンサ出力をインターフェース111を通じて取り込み、玄関ドア1が開けられた否か監視する（ステップS66）。そして、CPU101は、玄関ドア1が開けられずに所定時間、例えば10秒経過したかどうかを判別し（ステップS67）、10秒経過したと判別したときには、玄関ドア1を自動的に施錠状態に戻すようにする（ステップS68）。そして、CPU101は、内側LED22inを緑色で点滅して、玄関ドア1が施錠状態に戻ったことを報知する（ステップS69）。

【0155】

また、ステップS66で、ステップS58での開錠後、10秒以内に玄関ドア1が開かれたと判別したときには、CPU101は、ステップS52で取り込んだ識別情報で示される在宅者が外出をしたと認識して、当該識別情報を含む個人情報、外出者情報として監視制御装置3に転送する（ステップS70）。

【0156】

その後、CPU101は、ドア開閉センサ27のセンサ出力を参照して、玄関ドア1が閉じられたことを確認し（ステップS71）、玄関ドア1が閉じられた後、所定時間、例えば3秒経過したことを確認したら（ステップS72）、ドアロック機構駆動部112を駆動制御して、ドアロック機構28により玄関ドア1を施錠状態に復帰させるようにする（図19のステップS81）。そして、CPU101は、外側LED22exを緑色で点滅して、玄関ドア1が施錠状態に戻ったことを電子鍵装置40の使用者に報知する（ステップS82）。この外側LED22exの緑色点滅は、所定時間、例えば10秒間続けられる。

【0157】

その後、CPU101は、前記所定時間、例えば10秒経過したか否かを判別し

(ステップS83)、所定時間経過していないと判別したときには、ステップS51で通信が行われたと判別された電子鍵装置が、再度、外側電子鍵リード／ライト部21exと通信したか否か判別する(ステップS84)、通信がなされないと判別したときにはステップS83に戻る。

【0158】

そして、ステップS83で、電子鍵装置と外側電子鍵リード／ライト部21exとで通信が行われずに、前記所定時間経過したと判別したときには、CPU101は、内側電子鍵リード／ライト部21inに対して電子鍵装置がかざされたことにより開始された玄関ドアのロック制御動作が一段落したとして、図17のステップS51に戻る。

【0159】

また、ステップS84で、玄関ドア施錠復帰後、外側LED22exの緑色点滅が終了する所定時間経過する前に、ステップS51において通信が行われたと判別された電子鍵装置と外側電子鍵リード／ライト部21exとで通信が行われたと判別すると、ステップS61～S63で確認された戸締りを再確認する(ステップS85)。

【0160】

ステップS85で、戸締りがOKであると判別したときには、CPU101は、通信インターフェース121を通じてセキュリティモードをオンにする要求を監視制御装置3に送信する(ステップS86)。

【0161】

この要求に対しては、監視制御装置3は、そのときの在宅状況をチェックして、セキュリティレベルが図11に示したいずれのレベルとなるかを判定する。そして、監視制御装置3は、その判定の結果、セキュリティレベルがレベルDであるときには、セキュリティモードはオンにできないので、その旨をドアロック制御装置100に返し、セキュリティレベルがレベルD以外であるときには、セキュリティモードをオンにできるので、その旨をドアロック制御装置100に返す。

【0162】

ドアロック制御装置100のCPU101は、監視制御装置3からのセキュリティモードオンの要求に対する返答を解析して、セキュリティモードをオンにできるか否かを判別する（ステップS87）。そして、セキュリティモードがオンにできる旨の返答を監視制御装置3から受けたと判別したときには、CPU101は、外側スピーカ23exから、「セキュリティモードをオンにします」というメッセージを放音させる（ステップS88）。

【0163】

また、ステップS87で、セキュリティモードがオンにできない旨の返答を監視制御装置3から受けたと判別したときには、CPU101は、外側スピーカ23exから、「在宅者が存在するため、セキュリティモードをオンにはできません」というメッセージを放音させる（ステップS89）。その後、ステップS51に戻る。

【0164】

また、ステップS85で、窓が開いていて戸締りが完了していないと判別したときには、CPU101は、「窓が開いているため、セキュリティモードをオンにすることはできません」という警告メッセージを放音する（ステップS90）。そして、その後、ステップS51に戻る。

【0165】

[外側電子鍵リード／ライト部21exでの通信の場合；図20～図22]

ステップS51で、電子鍵装置40と通信が行われたのが外側電子鍵リード／ライト部21exであると判別したときには、CPU101は、家人が帰宅した場合あるいはその他の外にいる者の入室要求であるとして、以下のような処理を行なう。

【0166】

CPU101は、まず、家族情報メモリ120に記憶されている識別情報と、電子鍵装置40から受信した識別情報とを比較して、家族情報メモリ120に記憶されている識別情報の中に、電子鍵装置40から受信した識別情報と一致するものがあるかどうかにより、当該電子鍵装置40がドアロック装置2に登録された電子鍵装置であるか否かを判別して、当該電子鍵装置40についての認証を行

なう（ステップS101）。

【0167】

そして、その認証結果を判別し（ステップS102）、家族情報メモリ120に記憶されている識別情報の中に、電子鍵装置40から受信した識別情報と一致するものがなくて、認証が取れなかったとき（認証NG）であると判別したときには、CPU101は、外側LED駆動部108を駆動して、外側LED22exを赤色で点滅させると共に、外側スピーカ23exから警告音を放音して、認証NGであることを電子鍵装置40の使用者に報知する（ステップS103）。そして、ドアロック機構28は施錠状態のままとして、ステップS51に戻る。

【0168】

また、ステップS102で、家族情報メモリ120に記憶されている識別情報の中に、電子鍵装置40から受信した識別情報と一致するものがあって、認証がOKであると判別したときには、CPU101は、外側LED駆動部108を駆動して、外側LED22exを緑色で1秒間点灯させ、認証OKであることを電子鍵装置40の使用者に報知する（ステップS104）。このとき、CPU101により、合わせて外側スピーカ23exから「認証がとれました」というメッセージを放音させるようにしても良い。

【0169】

そして、このとき、認証がOKであることから、CPU101は、ドアロック機構駆動部112を駆動制御して、ドアロック機構28により玄関ドア1を開錠状態にし（ステップS105）、外側スピーカ23exから、「ドアロックを解除しました」というメッセージを放音させる（ステップS106）。このとき、外側LED22exを、例えば緑色で点滅させ、ドアロックの解除状態を電子鍵装置40の使用者に報知するようにしてもよい。

【0170】

次に、CPU101は、ドア開閉センサ27のセンサ出力をインターフェース111を通じて取り込み、玄関ドア1が開けられた否か監視する（ステップS107）。そして、CPU101は、玄関ドア1が開けられずに所定時間、例えば10秒経過したかどうかを判別し（ステップS108）、10秒経過したと判別

したときには、玄関ドア1を自動的に施錠状態に戻すようにする（ステップS109）。そして、CPU101は、外側LED22exを緑色で点滅して、玄関ドア1が施錠状態に戻ったことを報知する（ステップS110）。

【0171】

その後、CPU101は、所定時間、例えば10秒経過したか否か判別し（ステップS111）、所定時間経過していないと判別したときには、ステップS51で通信が行われたと判別された電子鍵装置が外側電子鍵リード／ライト部21exと通信したか否か判別し（ステップS112）、通信がなされないと判別したときにはステップS111に戻る。

【0172】

そして、ステップS111で、電子鍵装置と外側電子鍵リード／ライト部21exとで通信が行われずに、所定時間経過したと判別したときには、CPU101は、外側電子鍵リード／ライト部21exに対して電子鍵装置がかざされたことにより開始された玄関ドアのロック制御動作が一段落したとして、図17のステップS51に戻る。

【0173】

また、ステップS112で、玄関ドア施錠復帰後、所定時間経過する前に、ステップS51において通信が行われたと判別された電子鍵装置と外側電子鍵リード／ライト部21exとで通信が行われたと判別すると、戸締りを確認する（ステップS113）。

【0174】

このステップS113での戸締りの確認は、前述のステップS61～S63において説明した処理と同様に行なう。つまり、ドアロック制御装置100は、監視制御装置3に対して窓の開閉状態についての問い合わせを行ない、問い合わせ結果を監視制御装置3から取得する。そして、その問い合わせ結果から、戸締りがOKかどうかを判別する。

【0175】

ステップS113で、戸締りがOKであると判別したときには、CPU101は、通信インターフェース121を通じてセキュリティモードをオンにする要求

を監視制御装置 3 に送信する（ステップ S 1 1 4）。

【0176】

この要求に対しては、監視制御装置 3 は、そのときの在宅状況をチェックして、セキュリティレベルが図 1 1 に示したいずれのレベルとなるかを判定する。そして、監視制御装置 3 は、その判定の結果、セキュリティレベルがレベル D であるときには、セキュリティモードはオンにできないので、その旨をドアロック制御装置 1 0 0 に返し、セキュリティレベルがレベル D 以外であるときには、セキュリティモードをオンにできるので、その旨をドアロック制御装置 1 0 0 に返す。

【0177】

ドアロック制御装置 1 0 0 の CPU 1 0 1 は、監視制御装置 3 からのセキュリティモードオンの要求に対する返答を解析して、セキュリティモードをオンにできるか否かを判別する（ステップ S 1 1 5）。そして、セキュリティモードがオンにできる旨の返答を監視制御装置 3 から受けたと判別したときには、CPU 1 0 1 は、外側スピーカ 2 3 e x から、「セキュリティモードをオンにします」というメッセージを放音させる（ステップ S 1 1 6）。

【0178】

また、ステップ S 1 1 5 で、セキュリティモードがオンにできない旨の返答を監視制御装置 3 から受けたと判別したときには、CPU 1 0 1 は、外側スピーカ 2 3 e x から、「在宅者が存在するため、セキュリティモードをオンにはできません」というメッセージを放音させる（ステップ S 1 1 7）。その後、ステップ S 5 1 に戻る。

【0179】

また、ステップ S 1 1 3 で、窓が開いていて戸締りが完了していないと判別したときには、CPU 1 0 1 は、「窓が開いているため、セキュリティモードをオンにすることはできません」という警告メッセージを放音する（ステップ S 1 1 8）。そして、その後、ステップ S 5 1 に戻る。

【0180】

ステップ S 1 1 1 ～ステップ S 1 1 8 の処理は、一旦、玄関ドア 1 を内側から

開錠した後、所定時間以内に、外側電子鍵リード／ライト部 21ex に電子鍵装置をかざして、セキュリティモードをオンにするのを忘れた者が、もう一度、室内に戻って、内側電子鍵リード／ライト部 21in に対して電子鍵装置をかざすところからやり直す手間を防止するための処理である。

【0181】

すなわち、一旦、玄関ドア 1 を内側から開錠した後、所定時間以内に、外側電子鍵リード／ライト部 21ex に電子鍵装置をかざして、セキュリティモードをオンにするのを忘れた、あるいは失敗した場合に、外側電子鍵リード／ライト部 21ex に電子鍵装置をかざして、玄関ドア 1 を一旦開錠させ、その後、10秒待つて再施錠になった後、10秒以内に、再び、外側電子鍵リード／ライト部 21ex に電子鍵装置をかざすことにより、セキュリティモードをオンにすることができるものである。このようにすれば、セキュリティモードをオンに設定するために、開錠してから室内に入り、内側電子鍵リード／ライト部 21in に電子鍵装置 40 をかざすところからやり直す必要がなく、便利である。

【0182】

次に、ステップ S107 で、ステップ S105 での開錠後、10秒以内に玄関ドア 1 が開かれたと判別したときには、CPU101 は、ステップ S52 で取り込んだ識別情報で示される外出者が帰宅したと認識して、当該識別情報を含む個人情報情報を、帰宅者情報として監視制御装置 3 に転送する（図 22 のステップ S121）。

【0183】

その後、CPU101 は、ドア開閉センサ 27 のセンサ出力を参照して、玄関ドア 1 が閉じられたことを確認し（ステップ S122）、玄関ドア 1 が閉じられた後、所定時間、例えば 3 秒経過したことを確認したら（ステップ S123）、ドアロック機構駆動部 112 を駆動制御して、ドアロック機構 28 により玄関ドア 1 を施錠状態に復帰させるようにする（ステップ S124）。そして、CPU101 は、内側 LED 22in を緑色で点滅して、玄関ドア 1 が施錠状態に戻ったことを報知する（ステップ S125）。

【0184】

その後、CPU101は、帰宅者があったことから在宅状況が変更することに基づき、セキュリティレベルの変更指示を監視制御装置3に送る（ステップS126）。

【0185】

このセキュリティレベルの変更指示を受け取った監視制御装置3では、ステップS121での帰宅者情報による在宅状況の変化を認識し、図11に示した在宅状況とセキュリティレベルとの対応テーブルを参照して、セキュリティレベルの変更の必要があるか否か判別し、必要があるときには、セキュリティレベルを変更する。そして、監視制御装置3は、セキュリティレベルを変更したかどうかを、ドアロック制御装置100に通知する。

【0186】

ドアロック制御装置100のCPU101は、監視制御装置3からのセキュリティレベルの変更に関する通知を受け取って（ステップS127）、セキュリティレベルが変更されたか否かを判別する（ステップS128）。

【0187】

そして、ステップS128で、セキュリティモードが変更されたと判別したときには、CPU101は、内側スピーカ23inから、「セキュリティレベルを変更しました」というメッセージを放音する（ステップS129）。そして、ステップS51に戻る。

【0188】

なお、以上の説明では、帰宅者があったときには、ドアロック制御装置100から、ステップS126において、監視制御装置3にセキュリティレベルの変更指示を送るようにしたが、監視制御装置3では、ステップS121での帰宅者情報の転送を受けるので、ドアロック制御装置100からのセキュリティレベルの変更指示を受けなくても、自動的にセキュリティレベルの変更が必要かどうかを判断して、必要である場合には、セキュリティレベルを自動的に変更するようにしても良い。その場合には、セキュリティレベルを変更したときには、その旨をドアロック制御装置100に転送するようにする。

【0189】

[逐次ロックモードの説明；図23～図25]

次に、逐次ロックモードのときの動作を、図23～図25のフローチャートを参照しながら説明する。この逐次ロックモードのときには、電子鍵装置40が、内側電子鍵リード／ライト部21inまたは外側電子鍵リード／ライト部21exにかざされて通信が両者の間で行なわれ、電子鍵情報としての識別情報についての認証がとれたときには、そのときの玄関ドア1の開錠あるいは施錠の状態とは逆の状態になるように、ドアロック機構28は、ドアロック制御装置100により制御されるものである。

【0190】

CPU101は、インターフェース105、106を介して、内側電子鍵リード／ライト部21inおよび外側電子鍵リード／ライト部21exを監視し、電子鍵装置40がかざされて、電子鍵装置40と内側電子鍵リード／ライト部21inまたは外側電子鍵リード／ライト部21exとの間で通信が行われるのを待つ（ステップS131）。

【0191】

そして、ステップS131において、電子鍵装置40がかざされて、電子鍵装置40と通信が行なわれたと判別したときには、CPU101は、識別情報を電子鍵装置40から受信し、例えばRAM104などに一時的に格納する（ステップS132）。このとき、前述と同様に、電子鍵装置40には時刻情報等が書き込まれると共に、家族情報メモリ120および監視制御装置3の家族情報メモリ205への時刻情報等の書き込みが行なわれる。

【0192】

内側電子鍵リード／ライト部21inまたは外側電子鍵リード／ライト部21exのどちらで電子鍵装置40と通信が行われたかを判別する（ステップS133）。

【0193】

[内側電子鍵リード／ライト部21inでの通信の場合；図23]

ステップS133で、電子鍵装置40と通信が行われたのが内側電子鍵リード／ライト部21inであると判別したときには、CPU101は、在宅者が外出

する場合あるいは玄関ドア1をセキュリティのために施錠する場合であるとして、以下のような処理を行なう。

【0194】

CPU101は、先ず、家族情報メモリ120に記憶されている識別情報と、電子鍵装置40から受信した識別情報とを比較して、家族情報メモリ120に記憶されている識別情報の中に、電子鍵装置40から受信した識別情報と一致するものがあるかどうかにより、当該電子鍵装置40がドアロック装置2に登録された電子鍵装置であるか否かを判別して、当該電子鍵装置40についての認証を行なう（ステップS134）。

【0195】

そして、その認証結果を判別し（ステップS135）、家族情報メモリ120に記憶されている識別情報の中に、電子鍵装置40から受信した識別情報と一致するものがなくて、認証が取れなかったとき（認証NG）であると判別したときには、CPU101は、内側LED駆動部107を駆動して、内側LED22inを赤色で点滅させると共に、内側スピーカ23inから警告音を放音して、認証NGであることを電子鍵装置40の使用者に報知する（ステップS136）。そして、ドアロック機構28は、その前の状態のままとして、ステップS131に戻る。

【0196】

また、ステップS135で、家族情報メモリ120に記憶されている識別情報の中に、電子鍵装置40から受信した識別情報と一致するものがあって、認証がOKであると判別したときには、CPU101は、内側LED駆動部107を駆動して、内側LED22inを緑色で1秒間点灯させ、認証OKであることを電子鍵装置40の使用者に報知する（ステップS137）。このとき、CPU101により、併せて内側スピーカ23inから「認証がとれました」というメッセージを放音させるようにしても良い。

【0197】

そして、CPU101は、現在のドアロック機構28による玄関ドア1のロック状態は、施錠状態になっているか否かを判別する（ステップS138）。このス

ステップS138で、ドアロック機構28による玄関ドア1のロック状態が、開錠状態であると判別したときには、その逆の状態である施錠状態にするように、ドアロック機構駆動部112を駆動制御する（ステップS139）。

【0198】

そして、CPU101は、内側LED22inを、例えば緑色で点滅させると共に、内側スピーカ23inから、「玄関ドアを施錠しました」というメッセージを放音させ、施錠状態にしたことを電子鍵装置40の使用者に報知するようにする（ステップS140）。

【0199】

そして、CPU101は、ステップS132で取り込んだ識別情報で示される者が、セキュリティのために施錠をしたと認識して、当該識別情報を含む個人情報、在宅者情報として監視制御装置3に転送する（ステップS141）。

【0200】

また、ステップS138で、現在のドアロック機構28のロック状態は、施錠状態であると判別したときには、CPU101は、ドアロック機構駆動部112を駆動制御して、ドアロック機構28を開錠状態にし（ステップS142）、内側LED22inを、例えば緑色で点滅させると共に、内側スピーカ23inから、「ドアロックを解除しました」というメッセージを放音させる（ステップS143）。

【0201】

そして、このときには、CPU101は、ステップS132で取り込んだ識別情報で示される者が、開錠をして外出をしたと認識して、当該識別情報を含む個人情報を、外出者情報として監視制御装置3に転送する（ステップS144）。

【0202】

[外側電子鍵リード／ライト部21exでの通信の場合；図24～図25]

ステップS133で、電子鍵装置40と通信が行われたのが外側電子鍵リード／ライト部21exであると判別したときには、CPU101は、家人が帰宅して開錠する場合あるいは家人が外出のため施錠する場合であるとして、以下のような処理を行なう。

【0203】

CPU101は、まず、家族情報メモリ120に記憶されている識別情報と、電子鍵装置40から受信した識別情報とを比較して、家族情報メモリ120に記憶されている識別情報の中に、電子鍵装置40から受信した識別情報と一致するものがあるかどうかにより、当該電子鍵装置40がドアロック装置2に登録された電子鍵装置であるか否かを判別して、当該電子鍵装置40についての認証を行なう（ステップS151）。

【0204】

そして、その認証結果を判別し（ステップS152）、家族情報メモリ120に記憶されている識別情報の中に、電子鍵装置40から受信した識別情報と一致するものがなくて、認証が取れなかったとき（認証NG）であると判別したときには、CPU101は、外側LED駆動部108を駆動して、外側LED22exを赤色で点滅させると共に、外側スピーカ23exから警告音を放音して、認証NGであることを電子鍵装置40の使用者に報知する（ステップS153）。そして、ドアロック機構28は施錠状態のままとして、ステップS131に戻る。

【0205】

また、ステップS102で、家族情報メモリ120に記憶されている識別情報の中に、電子鍵装置40から受信した識別情報と一致するものがあって、認証がOKであると判別したときには、CPU101は、外側LED駆動部108を駆動して、外側LED22exを緑色で1秒間点灯させ、認証OKであることを電子鍵装置40の使用者に報知する（ステップS154）。このとき、CPU101により、併せて外側スピーカ23exから「認証がとれました」というメッセージを放音させるようにしても良い。

【0206】

そして、CPU101は、現在のドアロック機構28のロック状態は、施錠状態になっているか否かを判別する（ステップS155）。このステップS155で、現在のドアロック機構28による玄関ドア1のロック状態は、施錠状態であると判別したときには、CPU101は、ドアロック機構駆動部112を駆動制御

して、ドアロック機構 28 により玄関ドア 1 を開錠状態にし（ステップ S 156）、内側 LED 22 in を、例えば緑色で点滅させると共に、内側スピーカ 23 in から、「ドアロックを解除しました」というメッセージを放音させる（ステップ S 157）。

【0207】

そして、CPU 101 は、ステップ S 132 で取り込んだ識別情報で示される者が、帰宅のため開錠をしたと認識して、当該識別情報を含む個人情報を、帰宅者情報として監視制御装置 3 に転送する（ステップ S 158）。

【0208】

また、ステップ S 155 で、現在の玄関ドア 1 のロック状態が開錠状態であると判別したときには、その逆の状態である施錠状態にするように、ドアロック機構駆動部 112 を駆動制御して、ドアロック機構 28 により玄関ドア 1 を施錠状態にする（ステップ S 159）。

【0209】

そして、CPU 101 は、内側 LED 22 in を、例えば緑色で点滅させると共に、内側スピーカ 23 in から、「玄関ドアを施錠しました」というメッセージを放音させ、施錠状態にしたことを電子鍵装置 40 の使用者に報知するようにする（ステップ S 160）。

【0210】

そして、CPU 101 は、ステップ S 132 で取り込んだ識別情報で示される者が、外出のために施錠をしたと認識して、当該識別情報を含む個人情報を、外出者情報として監視制御装置 3 に転送する（ステップ S 161）。

【0211】

そして、施錠後、CPU 101 は、所定時間、例えば 10 秒経過したか否か判別し（図 25 のステップ S 162）、所定時間経過していないと判別したときには、ステップ S 131 で通信が行われたと判別された電子鍵装置が、再度、外側電子鍵リード／ライト部 21 ex と通信したか否か判別し（ステップ S 163）、通信がなされないと判別したときにはステップ S 162 に戻る。

【0212】

また、ステップ S 163 で、玄関ドア施錠後、所定時間経過する前に、ステップ S 51 において通信が行われたと判別された電子鍵装置と外側電子鍵リード／ライト部 21ex とで通信が行われたと判別すると、戸締りを確認する（ステップ S 164）。

【0213】

このステップ S 164 での戸締りの確認は、前述のステップ S 61～S 63 において説明した処理と同様に行なう。つまり、ドアロック制御装置 100 は、監視制御装置 3 に対して窓の開閉状態についての問い合わせを行ない、問い合わせ結果を監視制御装置 3 から取得する。そして、その問い合わせ結果から、戸締りが OK かどうかを判別する。

【0214】

ステップ S 164 で、戸締りが OK であると判別したときには、CPU 101 は、通信インターフェース 121 を通じてセキュリティモードをオンにする要求を監視制御装置 3 に送信する（ステップ S 165）。

【0215】

この要求に対しては、監視制御装置 3 は、そのときの在宅状況をチェックして、セキュリティレベルが図 11 に示したいずれのレベルとなるかを判定する。そして、監視制御装置 3 は、その判定の結果、セキュリティレベルがレベル D であるときには、セキュリティモードはオンにできないので、その旨をドアロック制御装置 100 に返し、セキュリティレベルがレベル D 以外であるときには、セキュリティモードをオンにできるので、その旨をドアロック制御装置 100 に返す。

【0216】

ドアロック制御装置 100 の CPU 101 は、監視制御装置 3 からのセキュリティモードオンの要求に対する返答を解析して、セキュリティモードをオンにできるか否か判別する（ステップ S 166）。そして、セキュリティモードがオンにできる旨の返答を監視制御装置 3 から受けたと判別したときには、CPU 101 は、外側スピーカ 23ex から、「セキュリティモードをオンにします」というメッセージを放音させる（ステップ S 167）。

【0217】

また、ステップS166で、セキュリティモードがオンにできない旨の返答を監視制御装置3から受けたと判別したときには、CPU101は、外側スピーカ23exから、「在宅者が存在するため、セキュリティモードをオンにはできません」というメッセージを放音させる（ステップS168）。その後、ステップS131に戻る。

【0218】

また、ステップS164で、窓が開いていて戸締りが完了していないと判別したときには、CPU101は、「窓が開いているため、セキュリティモードをオンにすることはできません」という警告メッセージを放音する（ステップS169）。そして、その後、ステップS131に戻る。

【0219】

〔監視制御装置3におけるセキュリティ動作；図26〕

上述のようにして、監視制御装置3は、ドアロック制御装置100からの指示を受けてセキュリティモードをオンにするが、リモートコマンド50のセキュリティボタン51を押すことによってもセキュリティモードをオンにすることができる。そして、監視制御装置3のセキュリティモードオン状態は、リモートコマンド50のオフボタン52を操作すると、オフとすることができる。

【0220】

図26は、リモートコマンド50を操作することにより、監視制御装置3のセキュリティモードのオン・オフを制御する動作を説明するためのフローチャートである。

【0221】

まず、CPU201は、リモートコマンド50からの遠隔操作信号を監視して、リモートコマンド50で操作入力となされたか否かを判別する（ステップS171）。そして、操作入力となされたと判別したときには、CPU201は、操作されたのはセキュリティボタン51であるか否かを判別する（ステップS172）。

。

【0222】

ステップS172での判別の結果、セキュリティボタン51の操作であると判別したときには、CPU201は、リモコン送信部39から電源オンのリモコン信号をテレビ受像機7のリモコン受信部に送り、テレビ受像機7をオンにする（ステップS173）。

【0223】

そして、CPU201は、ROM203から読み出したデータに基づいて生成した画像情報を、テレビインターフェース217を通じてテレビ受像機7に送り、テレビ受像機7の画面にセキュリティモードオンの確認画面を表示する（ステップS174）。その後、CPU201は、リモコン送信部39からテレビ受像機7の電源をオフするリモコン信号を送出して、テレビ受像機7をオフさせる（ステップS175）。

【0224】

そして、CPU201は、その所定時間、例えば5分経過後、セキュリティモードをオンにして（ステップS177）、セキュリティ監視動作を実行する（ステップS178）。ステップS177における所定時間は、セキュリティボタン51を操作した使用者が、セキュリティモードオンに設定した後、玄関ドアから退出するまでの時間を考慮した時間とされている。

【0225】

ステップS172において、リモートコマンド50で操作されたボタンがセキュリティボタン51ではないと判別したときには、CPU201は、操作されたのはオフボタン52であるか否かを判別する（ステップS179）。このステップS179でオフボタン52ではないと判別したときには、CPU201は、その他のボタンが押されたことによる処理を実行する（ステップS180）。

【0226】

ステップS179での判別の結果、オフボタン52であると判別したときには、CPU201は、リモコン送信部39から電源オンのリモコン信号をテレビ受像機7のリモコン受信部に送り、テレビ受像機7をオンにする（ステップS181）。

【0227】

そして、CPU 201は、ROM 203から読み出したデータに基づいて生成した画像情報を、テレビインターフェース 217を通じてテレビ受像機 7に送り、テレビ受像機 7の画面にセキュリティモードオフの確認画面を表示する（ステップ S182）。その後、CPU 201は、リモコン送信部 39からテレビ受像機 7の電源をオフするリモコン信号を送出して、テレビ受像機 7をオフさせる（ステップ S183）。

【0228】

そして、CPU 201は、セキュリティモードをオフにする処理を行なう（ステップ S184）。以上で、図 26の処理ルーチンは終了となる。

【0229】

[セキュリティモードオンにおける監視動作]

図 27および図 28は、監視制御装置 3において、セキュリティモードオンとされたときの処理動作である。これは、前述のリモートコマンド 50でのセキュリティボタン 51の操作時に起動されるもので、このときのセキュリティレベルは、レベル Aの場合である。なお、ドアロック制御装置 100からのセキュリティモードオン指示があったときには、前述したように、在宅者の状況が参酌されてセキュリティレベルが決定され、その決定されたセキュリティレベルでセキュリティモードがオンとされるものである。

【0230】

図 27においては、まず、CPU 201は、ビデオカメラ 31の撮影画像の取り込みを開始する（ステップ S191）。このとき、マイクロホン 34で収音した音声も一緒に取り込みを行なう。前述したように、画像・音声メモリ 208に設けられるセキュリティモード用の監視情報領域は、リングバッファ形式とされており、この例では、最新の 30秒分の画像・音声情報が常に画像・音声メモリ 208に格納されるようにされている。監視カメラ 13からの撮影画像についても同様にされている。

【0231】

次に、CPU 201は、センサハブ 207からの窓センサ 16a、16bのセンサ出力と、玄関ドア 1のドア開閉センサ 27のセンサ出力の監視を開始するよ

うに制御する（ステップS192）。さらに、CPU201は、火災センサ4およびガスセンサ5のセンサ出力の監視を開始するように制御する（ステップS193）。監視カメラ13は、火災センサ4やガスセンサ5のオン・オフに応じてオン・オフする。

【0232】

次に、CPU201は、人感センサ33のセンサ出力を監視して、侵入者がいかどうかチェックする（ステップS194）。侵入者なしと判別したときには、窓センサ16a、16bのセンサ出力や、ドア開閉センサ27のセンサ出力から、異常を検知したか否か判別する（ステップS211）。

【0233】

ステップS211で、異常を検知しないと判別したときには、CPU201は、火災センサ4やガスセンサ5のセンサ出力から、異常を検知したか否か判別する（ステップS212）。ステップS212で、異常を検知しないと判別したときには、ステップS194に戻る。

【0234】

そして、ステップS194で、侵入者を人感センサ33により検知したと判別したときには、CPU201は、照明機構320を制御して、照明32をオンにする（ステップS195）。そして、侵入者の検知時点の10秒前から、検知時点の20秒後までの30秒分の画像・音声情報を、画像・音声メモリ208から読み出し、1回目の画像として、管理サーバ装置10に転送する（ステップS196）。管理サーバ装置10では、この転送されてきた画像・音声情報により、侵入者を認識して、適切な処置を取ることができる。

【0235】

次に、CPU201は、リモコン送信部39からテレビ受像機7に電源オンのリモコン信号を送り、テレビ受像機7をオンにする（ステップS197）。そして、CPU201は、予め用意している威嚇画像および威嚇音声の情報をテレビ受像機7に送り、それら威嚇画像および威嚇音声を出力する（ステップS198）。この威嚇画像・音声により侵入した賊を威嚇して、退散させることが可能となる。

【0236】

次に、CPU201は、監視制御装置3に予め登録されている連絡先、例えば警備会社、警察署の他、登録された家人の携帯電話に対して異常検知を連絡する（ステップS199）。

【0237】

そして、CPU201は、その後、数秒間隔で、画像・音声メモリ208のリングバッファに格納されている30秒分の画像・音声情報を繰り返し管理サーバ装置10に転送する（ステップS200）。そして、CPU201は、人感センサ33が侵入者を検知しなくなったか否か判別し（ステップS201）、検知しなくなるまで、30秒分の画像・音声情報を管理サーバ装置10に転送する処理作業を継続する。

【0238】

そして、CPU201は、人感センサ33が侵入者を検知しなくなったと判別したときには、30秒分の画像・音声情報の管理サーバ装置10への転送を中止する（ステップS202）。そして、ステップS191に戻って、セキュリティ監視を続ける。

【0239】

また、ステップS211において、異常を検知したと判別したときには、CPU201は、窓センサ6a、6bやドア開閉センサ27の近傍に設置されている監視カメラ13からの検知時点の10秒前から、検知時点の20秒後までの30秒分画像を1回目として、管理サーバ装置10に転送する（ステップS214）。

【0240】

そして、CPU201は、リモコン送信部39からテレビ受像機7に電源オンのリモコン信号を送り、テレビ受像機7をオンにする（ステップS215）。そして、CPU201は、予め用意している威嚇画像および威嚇音声の情報をテレビ受像機7に送り、それら威嚇画像および威嚇音声を出力する（ステップS216）。この威嚇画像・音声により侵入した賊を威嚇して、退散させることが可能となる。

【0241】

次に、CPU201は、監視制御装置3に予め登録されている連絡先、例えば警備会社、警察署の他、登録された家人の携帯電話に対して異常検知を連絡する（ステップS217）。

【0242】

そして、CPU201は、その後、数秒間隔で、画像・音声メモリ208のリングバッファに格納されている30秒分の画像・音声情報を繰り返し管理サーバ装置10に転送する（ステップS218）。そして、CPU201は、リモートコマンド50のオフボタン52によるオフ指示を待ち（ステップS219）、オフ指示が有ったときには、セキュリティモードをオフとする。

【0243】

また、ステップS212で、火災センサ4またはガスセンサ5で異常が検知されたと判別したときには、CPU201は、監視制御装置3に設定登録されている、例えば警備会社、消防署の他、登録された家人の携帯電話に対して異常検知を連絡する（ステップS213）。そして、ステップS219に進む。

【0244】

なお、画像・音声情報を監視制御装置3から受け取った管理サーバ装置10は、Webページにそれらの画像・音声情報を載せる。そこで、監視制御装置3から連絡を受け取った携帯電話の持ち主は、管理サーバ装置10の当該Webページにアクセスして、どのような異常が発生したかを知ることができ、適切な対応処置を講じることが可能になる。

【0245】

[監視制御装置3におけるドアロック制御装置100からの指示による連携；
図29]

監視制御装置3のCPU201は、ドアロック制御装置100から受け取った情報や指示に応じて、図29に示すような連携動作を行なう。なお、この例は、セキュリティレベルの変更は、CPU201が、ドアロック制御装置100からの変更指示を受けて行なうのではなく、ドアロック制御装置100からの個人情報を受け取った結果による在宅状況の変化をチェックして、必要に応じて行なう

ようにした場合である。

【0246】

すなわち、CPU201は、ドアロック制御装置100からセキュリティモードオンの指示を受け取ったか否か判別する（ステップS221）。受け取らないと判別したときには、CPU201は、その他の処理を行なう（ステップS222）。

【0247】

ステップS221でセキュリティモードオンの指示を受信したと判別したときには、CPU201は、家族情報メモリ205の記憶情報を参照して、在宅状況をチェックする（ステップS223）。そして、図11に示したテーブルを参照して、在宅状況に応じたセキュリティレベルを認識し、セキュリティモードオンにすることが可能であるか否か判別する（ステップS224）。

【0248】

ステップS224で、セキュリティモードオンにすることができないと判別したときには、CPU201は、その旨をドアロック制御装置100に通知する（ステップS225）。

【0249】

一方、ステップS224で、セキュリティモードオンにすることが可能であると判別したときには、セキュリティモードをオンにすることができる旨をドアロック制御装置100に通知し（ステップS226）、所定時間経過するのを待つ（ステップS227）。

【0250】

所定時間経過したことを確認したら、CPU201は、在宅状況に応じたセキュリティレベルでセキュリティモードをオンにする（ステップS228）。そして、セキュリティ監視動作を開始する（ステップS229）。

【0251】

このセキュリティ監視動作中において、ドアロック制御装置100から識別情報を含む個人情報を受信したか否か判別し（ステップS230）、受信しなければステップS229に戻って、セキュリティ監視動作を継続する。ドアロック制

御装置 100 から個人情報を受信したと判別したときには、その結果としての在宅状況の変化をチェックし（ステップ S 231）、セキュリティレベルの変更が必要であるか判別する（ステップ S 232）。

【0252】

セキュリティレベルの変更が必要ではないと判別したときには、CPU 201 は、ステップ S 229 に戻って、セキュリティ監視動作を継続する。また、ステップ S 232 で、セキュリティレベルの変更が必要であると判別したときには、変更の結果、セキュリティモードはオフにすべきものであるか否か判別し（ステップ S 233）、そうではないときには、在宅状況に応じてセキュリティレベルを変更する（ステップ S 234）。そして、セキュリティレベルを変更した旨をドアロック制御装置 100 に通知する（ステップ S 235）。

【0253】

また、ステップ S 233 で、セキュリティモードはオフにすべきものであると判別したときには、セキュリティモードをオフにし（ステップ S 236）、その旨をドアロック制御装置 100 に通知する（ステップ S 237）。そして、ステップ S 221 に戻る。

【0254】

以上のようにして、この実施形態によれば、非接触の電子鍵装置を用いて、施錠、開錠を行なうので、鍵穴がなく、いわゆるピッキング対策の防犯効果がある。

【0255】

また、ドアロック装置 2 を、オートロックモードと、逐次ロックモードとで使い分けることができるので、使用者が、自分の使い勝手に合わせて、いずれのモードにするかを選択することができて、非常に便利である。

【0256】

また、内側電子鍵リード／ライト部 21in を設けて、この内側電子鍵リード／ライト部 21in によっても、ドアのロック状態を電子鍵装置により制御することができるので、窓などから侵入した不審者が玄関ドアから退出するのを妨げることができる。

【0257】

また、内側電子鍵リード／ライト部 21in と、外側電子鍵リード／ライト部 21ex とを設けることにより、これらと電子鍵装置との通信により、家族の入退出の管理をすることが容易である。

【0258】

そのため、ドアロック装置 2 と、監視制御装置 3 とを組み合わせることにより、効率的なセキュリティ管理をすることができるようになる。そして、セキュリティモードをドアロック時に設定できるようにしているので、従来は、家の中で設定して、所定時間後に、家の外に出なければならないなどのあわただしさを解消することができる。

【0259】

また、窓の閉め忘れがあったときには、ドアの開閉時に確認されるので、窓の閉め忘れを防止することができる。

【0260】

また、家人の年齢、性別などにより、セキュリティモードのレベルを可変することができるようにしたので、在宅者が弱者である場合にも効果的なセキュリティレベルを設定することができる。また、ドアロックの開錠、施錠に連携して、在宅状況の変化を把握することにより、セキュリティレベルの変更をすることができるというメリットもある。

【0261】**[電子鍵装置の電子鍵情報の登録]**

この電子鍵情報としての識別情報の登録が簡単にできることはセキュリティの点で好ましくないので、この例では、この電子鍵情報としての識別情報の登録は、次のようにセキュリティを重視した方法により、例えばドアロック装置 2 の販売業者あるいは設置業者もしくは使用者により行なわれる。

【0262】

先ず、本鍵情報の登録について説明する。この実施形態においては、前述したように、初期的な本鍵情報となる識別情報を記憶する電子鍵装置は、ICカードとしており、ドアロック装置 2 の販売業者あるいは設置業者から、ドアロック装

置 2 の各戸への設置に際して、使用者に渡される。

【0263】

この実施形態の場合、ドアロック装置 2 の各戸への設置前に、当該ドアロック装置 2 を設置する戸の家族構成員の各人についての個人情報が収集される。そして、当該家族構成員の各人に対して、本鍵情報となる識別情報を記憶する IC カードが割り当てられ、それぞれの IC カードに記憶される本鍵情報としての識別情報と、前記収集された個人情報とからなる個人プロフィール情報が構成される。

【0264】

そして、設置されるドアロック装置 2 のシリアル番号等からなる製品番号、設置される住所、電話番号、ドアロック装置を利用する家族構成員の氏名などのユーザ情報と、各家族構成員の前記個人プロフィール情報が、予め管理サーバ装置 10 のドアロック装置管理データベース 305 に、記憶される。すなわち、家族構成員それぞれの本鍵情報は、各家族構成員の個人プロフィール情報と関連付けられて予め管理サーバ装置 10 に登録されている。

【0265】

管理サーバ装置 10 に登録された本鍵情報および各家族構成員の個人プロフィール情報は、ドアロック装置 2 の設置業者や販売業者が、ドアロック装置 2 の設置を完了したときに、管理会社の管理サーバ装置 10 に初期登録要求をしたときに、管理サーバ装置 10 から監視制御装置 3 に転送されることにより、監視制御装置 3 の家族情報メモリ 205 に書き込まれて登録される。また、監視制御装置 3 に登録された情報のうち、少なくとも本鍵情報は、ドアロック制御装置 100 に転送されることにより、その家族情報メモリ 120 登録される。

【0266】

図 30 は、初期登録要求を受けたときの管理サーバ装置 10 の動作を示すものである。図 30 の各ステップの動作は、主として CPU 301 が主体となって行なうものである。

【0267】

先ず、CPU 301 は、初期登録要求を受け付けたか否かを判別する（ステップ

S 2 4 1)。この初期登録要求は、ドアロック装置 2 のシリアル番号等の装置識別情報を伴ったものとされているもので、例えばパーソナルコンピュータなどから通信ネットワークを通じて管理サーバ装置 1 0 に送られる場合と、電話等で、初期登録要求を受けたオペレータが図示しない入力手段により入力する場合とがある。

【0 2 6 8】

C P U 3 0 1 は、この初期登録要求を受け取ると、装置識別情報を検索子として、ドアロック装置データベースを検索し、予め登録されている電話番号を読み出して、初期登録要求を含む発呼をする。つまり、初期登録要求されたドアロック装置 2 が接続されている監視制御装置 3 に対して初期登録要求の発呼を行なう（ステップ S 2 4 2）。

【0 2 6 9】

このとき、監視制御装置 3 は、自動応答を行なうので、C P U 3 0 1 は、当該監視制御装置 3 からの応答を確認して、当該監視制御装置 3 との間に通信路を形成する（ステップ S 2 4 3）。

【0 2 7 0】

次に、C P U 3 0 1 は、ドアロック装置 2 に関連して上述のように管理サーバ装置 1 0 のドアロック装置データベース 2 0 5 に記憶している、ドアロック装置が設置された家の家族構成員全員についての本鍵情報を含む個人プロフィール情報を監視制御装置 3 に送信する（ステップ S 2 4 4）。

【0 2 7 1】

次に、C P U 3 0 1 は、監視制御装置 3 に送信すべき情報が全部終了し終わり、監視制御装置 3 から登録完了通知が到来するのを待ち（ステップ S 2 4 5）、登録完了通知を受け取ったと判別したときには、監視制御装置 3 との通信路を切断して（ステップ S 2 4 6）、この初期登録の処理ルーチンを終了する。

【0 2 7 2】

この初期登録要求情報を受け取る監視制御装置 3 の動作を、図 3 1 のフローチャートを参照して説明する。

【0 2 7 3】

監視制御装置 3 の CPU 201 は、管理サーバ装置 10 からの着信を受信したか否か判別し（ステップ S 251）、管理サーバ装置 10 からの着信の受信でなかったと判別したときには、その他の処理を行なう（ステップ S 252）。

【0274】

管理サーバ装置 10 からの着信を受信したと判別したときには、CPU 201 は、その着信に自動応答して管理サーバ装置 10 との間に通信路を形成する（ステップ S 253）。そして、受信した着信は初期登録要求であるか否か判別する（ステップ S 254）。初期登録要求であると判別すると、CPU 201 は、管理サーバ装置 10 からの登録情報を待ち、登録情報を受信したら（ステップ S 255）、受信した登録情報を、家族情報メモリ 205 に書き込む（ステップ S 256）。

【0275】

そして、家族全員についての登録情報の書き込みが完了したら、管理サーバ装置 10 に登録完了通知を返送し（ステップ S 257）、管理サーバ装置 10 との通信路を切断する（ステップ S 258）。

【0276】

次に、CPU 201 は、家族情報メモリ 205 に書き込んで登録した個人情報ファイル情報のうち、少なくとも家族構成員のそれぞれについての本鍵情報である識別情報をドアロック制御装置 100 に転送する（ステップ S 259）。ドアロック制御装置 100 は、この情報を受けて、家族情報メモリ 120 に受信した本鍵情報を登録する。本鍵情報としての識別情報のほかに、家族構成員についての個人情報の必要なものをも、ドアロック制御装置 100 に転送するようにしてもよいことは言うまでもない。なお、ドアロック制御装置 100 での登録動作は、上述の監視制御装置での鍵登録動作と同様であるので、ここでは省略する。

【0277】

そして、CPU 201 は、ドアロック制御装置 100 への本鍵情報および必要は情報の転送の終了を確認すると（ステップ S 260）、この処理ルーチンを終了する。

【0278】

なお、ステップ S 2 5 4 で、初期登録ではないと判別したときには、CPU 2 0 1 は、後述するバックアップ鍵の登録要求であるか否か判別し（ステップ S 2 6 1）、バックアップ鍵の登録要求であると判別したときには、当該バックアップ登録の処理を実行する（ステップ S 2 6 2）。このバックアップ登録の処理については後述する。

【0279】

また、ステップ S 2 6 1 でバックアップ登録要求ではないと判別したときには、CPU 2 0 1 は、紛失鍵の抹消要求であるか否か判別する（ステップ S 2 6 3）。そして、紛失鍵の抹消要求でないとは判別したときには、CPU 2 0 1 は、その他の処理を実行し（ステップ S 2 6 4）、紛失鍵の抹消要求であると判別したときには、当該抹消要求の処理を実行する（ステップ S 2 6 5）。以上で、図 3 1 の処理を終了する。

【0280】

[バックアップ鍵登録について]

この実施形態においては、管理サーバ装置 1 0 が備える鍵登録ホームページにアクセスすることにより、バックアップ鍵の登録を行なうことができる。図 3 2 は、このバックアップ鍵登録の際のシステム構成を説明するための図である。また、図 3 3 および図 3 4 は、このときの管理サーバ装置 1 0 の動作を説明するためのフローチャートである。

【0281】

図 3 2 に示すように、まず、電子鍵リード／ライト装置 2 0 0 1 を備える、あるいは電子鍵リード／ライト装置 2 0 0 1 が接続されているパーソナルコンピュータ 2 0 0 2 を用意する。そして、電子鍵リード／ライト装置 2 0 0 1 にバックアップ鍵として登録したい電子鍵装置、例えば IC カード、携帯電話端末、PDA をセットする。これらの電子鍵装置は、前述したように、本鍵情報が格納された IC カード 4 0 C の識別情報と異なるように一元管理された IC チップおよび電磁誘導アンテナなどからなる通信手段を備えるものである。

【0282】

次に、パーソナルコンピュータ 2 0 0 2 からインターネット 2 0 0 3 を通じて

管理サーバ装置 10 の鍵登録ホームページにアクセスする。

【0283】

管理サーバ装置 10 では、この鍵登録ホームページへのアクセスの有無を監視しており（ステップ S 271）、アクセスがないときには、その他の処理を行っている（ステップ S 272）。そして、鍵登録ホームページへのアクセスを受信したときには、CPU 301 は、鍵登録ホームページの表示情報を送信する（ステップ S 273）。

【0284】

この鍵登録ホームページは、パーソナルコンピュータ 2002 の画面に表示される。この画面には、登録者の認証確認用情報の入力を促すメッセージと、入力欄が表示されているので、予め定められたパスワードや顧客 ID、ドアロック装置 2 が設置された住所、電話番号、鍵登録を要求している者の氏名などの必要な認証確認用情報を入力した後、当該認証確認用情報を管理サーバ装置 10 に送る。

【0285】

管理サーバ装置 10 では、この認証確認用情報を受信したか否か判別し（ステップ S 274）、受信したら認証が OK であるか否か判別する（ステップ S 275）。認証が取れなかったとき（認証 NG のとき）には、認証 NG を報知する画面をパーソナルコンピュータ 2002 に送る（ステップ S 276）。

【0286】

この認証 NG を報知する画面では、認証確認用情報の再入力を行うことができると共に、アクセスを中断することもできる。鍵登録者は、いずれかの操作を行うことになる。

【0287】

そこで、管理サーバ装置 10 の CPU 301 は、認証確認用の情報を再受信したか否か判別し（ステップ S 277）、再受信しなかったときには、アクセスが中断されたかどうか判別し（ステップ S 278）、アクセス中断と判別されなかったときには、ステップ S 277 に戻る。そして、ステップ S 277 で、認証確認用の情報を再受信したと判別したときには、CPU 301 は、ステップ S 27

5に戻って、認証が取れるかどうか判別する。ステップS278で中断であると判別したときには、アクセス切断処理を行なう（ステップS279）。

【0288】

ステップS275において、認証がOKであると判別したときには、CPU301は、バックアップ鍵登録用画面を送信する（ステップS281）。このバックアップ鍵登録用画面には、鍵登録ボタンと、アクセス中断ボタンがある。鍵登録者は、いずれかのボタンを操作することになる。鍵登録ボタンが押されたときには、パーソナルコンピュータ2002は、バックアップ登録したい電子鍵装置40Bから電子鍵リード／ライト部2001により識別情報を読み取って、バックアップ鍵情報として管理サーバ装置10に送る。

【0289】

そこで、管理サーバ装置10のCPU301は、バックアップ鍵情報を受信したか否か判別し（ステップS282）、受信しなかったときには、アクセスが中断されたかどうか判別し（ステップS283）、アクセス中断と判別されなかったときには、ステップS282に戻る。

【0290】

そして、ステップS283で中断であると判別したときには、アクセス切断処理を行なって（ステップS279）、鍵ホームページを閉じる。また、ステップS282で、バックアップ鍵情報を受信したと判別したときには、CPU301は、ドアロック装置データベース305に、鍵登録要求者のバックアップ鍵情報として、受信した電子鍵情報を登録する（ステップS285）。このとき、電子鍵登録・紛失履歴メモリ306にも、その登録したバックアップ鍵情報と、鍵登録要求者の識別情報とがバックアップ登録履歴として、カレンダー情報および時刻情報と共に書き込まれる。

【0291】

そして、アクセス切断を行なった後（ステップS286）、鍵登録要求者が登録されているドアロック装置2が接続されている監視制御装置3に、バックアップ鍵登録要求の発信を行なう（ステップS287）。監視制御装置3では、このバックアップ鍵登録要求の発信の着信を受けると、その着信に自動応答するので

、CPU301は、当該監視制御装置3との間に通信路を形成する（ステップS288）。

【0292】

次に、CPU301は、鍵登録要求者を識別する情報と、バックアップ鍵情報とを監視制御装置3に送信する（ステップS289）。次に、CPU301は、監視制御装置3に送信すべき情報が全部終了し終わり、監視制御装置3から登録完了通知が到来するのを待ち（ステップS290）、登録完了通知を受け取ったと判別したときには、監視制御装置3との通信路を切断して（ステップS291）、このバックアップ鍵登録の処理ルーチンを終了する。

【0293】

次に、前記ステップS287～ステップS289での送信動作により管理サーバ装置10から送られてくるバックアップ鍵情報を受け取る監視制御装置3の動作を、図35のフローチャートを参照して説明する。この処理ルーチンは、図31におけるステップS262の処理に相当する。

【0294】

監視制御装置3のCPU201は、まず、バックアップ鍵情報と、鍵登録要求者の名前などの識別情報とを受信し（ステップS301）、鍵登録要求者を認識する（ステップS302）。次に、受信したバックアップ鍵情報を、認識した登録要求者のバックアップ鍵情報として、家族情報メモリ205に書き込んで登録する（ステップS303）。

【0295】

このとき、当該鍵登録要求者の個人プロフィール情報の電子鍵登録・紛失履歴エリアに、その登録したバックアップ鍵情報とカレンダー情報および時刻情報とがバックアップ登録履歴として書き込まれる。

【0296】

そして、CPU201は、管理サーバ装置10に、バックアップ鍵情報の登録完了通知を送る（ステップS304）。そして、管理サーバ装置10との通信路を切断する（ステップS305）。

【0297】

次に、CPU201は、家族情報メモリ205に書き込んで登録したバックアップ鍵情報である識別情報を、鍵登録要求者の識別情報と共に、ドアロック制御装置100に転送する（ステップS306）。ドアロック制御装置100は、この情報を受けて、家族情報メモリ120に、受信したバックアップ鍵情報を登録する。そして、CPU201は、ドアロック制御装置100への本鍵情報および必要は情報の転送の終了を確認すると（ステップS307）、この処理ルーチンを終了する。

【0298】

なお、ドアロック制御装置100における電子鍵情報の認証には本鍵情報のみを用いるようにする場合には、ステップS306およびステップS307の処理は、行なわなくてもよい。つまり、ドアロック制御装置100には、常に本鍵情報が存在すればよいからである。その場合には、後述する紛失鍵抹消登録の際に、紛失鍵情報の抹消と共に、新たに本鍵情報として使用する、予め監視制御装置3にバックアップ登録されていた鍵情報が、監視制御装置3からドアロック制御装置100に転送されるようにされる。

【0299】

なお、ドアロック制御装置100での登録動作は、上述の監視制御装置での鍵登録動作と同様であるので、ここでは省略する。

【0300】

なお、以上の電子鍵情報としての識別情報の登録動作は一例であって、例えばパーソナルコンピュータ2002および電子鍵リード／ライト装置2001の代わりに、監視制御装置3を用いて、同様にして管理サーバ装置10にアクセスして、バックアップ鍵を登録するようにしても良い。

【0301】

また、管理サーバ装置10を介することなく、監視制御装置3およびドアロック制御装置100に、電子鍵情報としての識別情報を登録することができるようにしても良い。

【0302】

なお、バックアップ鍵登録の際の鍵登録者の認証のために、本鍵情報を管理サ

ーバ装置に送り、その後、バックアップ鍵登録したい電子鍵装置をセットして登録を行なうようにしてもよい。その場合には、鍵登録者の認証は、本鍵情報により行なうことができるので、上述の例における鍵登録者の認証確認用情報の入力
は不要となる。

【0303】

[鍵の紛失対策]

電子鍵装置を紛失してしまった場合には、当該紛失した電子鍵装置の悪意の取得者の利用を防止するため、この実施形態では、電子鍵情報の抹消処理を行なうようにする。図36は、本鍵情報の抹消処理を行なう場合のシステム構成を示す図である。また、図37は、そのときの処理手順を説明するためのフローチャートである。

【0304】

まず、紛失者は、管理会社に対して紛失届を提出する（手順S311）。この紛失届は、電話やメールなどが用いられて行なわれる。この際に、紛失者の本人確認が行なわれ（手順S312）、本人確認がOKであったときに、紛失届が受理される（手順S313）。本人確認は、住所、氏名、年齢、電話番号、パスワード、顧客番号などにより行なわれる。

【0305】

次に、管理会社のオペレータは、管理サーバ装置10に対して紛失鍵情報の抹消処理およびバックアップ鍵情報の本鍵情報への格上げの処理を行なう（手順S314）。管理サーバ装置10のCPU301は、紛失鍵情報の抹消処理およびバックアップ鍵情報の本鍵情報への格上げの処理を完了すると、電子鍵登録・紛失履歴メモリ306に、その抹消したバックアップ鍵情報と、抹消要求者の識別情報とを、電子鍵抹消履歴として、カレンダー情報および時刻情報と共に書き込む。

【0306】

また、管理サーバ装置10のCPU301は、紛失鍵情報の抹消処理およびバックアップ鍵情報の本鍵情報への格上げの処理、抹消履歴の書き込みを完了すると、鍵紛失届を出した者が登録されているドアロック装置2が接続されている監

視制御装置 3 を、データベース 305 から検索して、自動的に、当該監視制御装置 3 にアクセスして、紛失鍵の抹消要求を送る（手順 S315）。

【0307】

紛失鍵の抹消要求を受信した監視制御装置 3 は、紛失鍵情報の抹消処理およびバックアップ鍵情報の本鍵情報への格上げの処理を行なう。そして、監視制御装置 3 は、紛失鍵情報の抹消処理およびバックアップ鍵情報の本鍵情報への格上げの処理を完了すると、個人プロフィール情報の電子鍵登録・抹消履歴エリアに抹消履歴を書き込み、その後、ドアロック装置 2 に対して紛失鍵の抹消指示をする。そして、バックアップ鍵が登録されていれば、当該バックアップ鍵の格上げ処理も指示する（手順 S316）。

【0308】

ドアロック装置 2 は、指示に従い、紛失鍵情報の抹消およびバックアップ鍵情報の格上げ処理を実行する（手順 S317）。

【0309】

なお、前述もしたように、ドアロック制御装置 100 における電子鍵情報の認証には本鍵情報のみを用いるようにする場合には、バックアップ鍵は、ドアロック制御装置 100 には登録されない。その場合には、手順 S316 では、紛失鍵の抹消指示と共に、監視制御装置 3 にバックアップ登録されている鍵情報を本鍵情報として、ドアロック制御装置 100 に送る。

【0310】

そして、その場合、ドアロック制御装置 100 では、手順 S317 において、抹消指示を受けた鍵情報を抹消すると共に、その代わりに新たに受信した本鍵情報の登録を行なうことになる。

【0311】

図 38 を参照して、手順 S314 および手順 S315 における管理サーバ装置 10 の動作を説明する。

【0312】

管理会社のオペレータは、管理サーバ装置 10 に対して紛失鍵の抹消要求者に関する情報を入力して、紛失鍵の抹消要求を入力する。管理サーバ装置 10 の C

P U 3 0 1 は、この紛失鍵の抹消要求が入力されたか否か判別する（ステップ S 3 2 1）。C P U 3 0 1 は、抹消要求がなければ、その他の処理を行なう（ステップ S 3 2 2）。

【0313】

ステップ S 3 2 1 で、紛失鍵の抹消要求が入力されたと判別したときには、C P U 3 0 1 は、ドアロック装置データベース 3 0 5 において抹消要求者および紛失鍵の情報を検索し（ステップ S 3 2 3）、抹消要求者の紛失鍵の情報を抹消すると共に、前述したように、電子鍵登録・紛失履歴メモリ 3 0 6 に紛失者および紛失鍵の情報を書き込む（ステップ S 3 2 4）。

【0314】

次に、C P U 3 0 1 は、抹消要求者の電子鍵情報としては、バックアップ鍵情報が登録されているかどうか判別し（ステップ S 3 2 5）、バックアップ鍵情報が登録されていると判別したときには、登録されているバックアップ鍵情報を本鍵情報に登録しなおす（ステップ S 3 2 6）。そして、抹消要求者が登録されている監視制御装置 3 を、データベース 3 0 5 から検索して、当該監視制御装置 3 に紛失鍵の抹消要求の発信を行なう（ステップ S 3 2 7）。ステップ S 3 2 5 で、バックアップ鍵情報が登録されていないと判別したときには、ステップ S 3 2 7 に即座に進む。

【0315】

監視制御装置 3 では、このバックアップ鍵登録要求の発信の着信を受けると、その着信に自動応答するので、C P U 3 0 1 は、当該監視制御装置 3 との間に通信路を形成する（ステップ S 3 2 8）。

【0316】

次に、C P U 3 0 1 は、抹消要求者を識別する情報と、抹消すべき紛失鍵の情報とを監視制御装置 3 に送信する（ステップ S 3 2 9）。次に、C P U 3 0 1 は、監視制御装置 3 に送信すべき情報が全部終了し終わり、監視制御装置 3 から抹消完了通知が到来するのを待ち（ステップ S 3 3 0）、抹消完了通知を受け取ったと判別したときには、監視制御装置 3 との通信路を切断して（ステップ S 3 3 1）、この紛失鍵情報の抹消処理ルーチンを終了する。

【0317】

次に、前記手順S316において、管理サーバ装置10から送られてくる紛失鍵の抹消要求を受け取ったときの監視制御装置3の動作を、図39のフローチャートを参照して説明する。この処理ルーチンは、図31におけるステップS265の処理に相当する。

【0318】

監視制御装置3のCPU201は、まず、紛失鍵情報と、抹消要求者の名前などの識別情報とを受信し（ステップS341）、抹消要求者および紛失鍵情報を認識する（ステップS342）。次に、認識した抹消要求者の紛失鍵情報を、家族情報メモリ205から抹消する（ステップS343）。そして、抹消要求者の個人プロフィール情報中の電子鍵登録・抹消履歴情報として、抹消した電子鍵情報としての識別情報および日付、時刻等を、家族情報メモリ205に書き込んだ後、管理サーバ装置10に、抹消完了通知を送る（ステップS344）。そして、管理サーバ装置10との通信路を切断する（ステップS345）。

【0319】

次に、CPU201は、抹消要求者の電子鍵情報としては、バックアップ鍵情報が登録されているかどうか判別し（ステップS346）、バックアップ鍵情報が登録されていると判別したときには、登録されているバックアップ鍵情報を本鍵情報に登録しなおす（ステップS347）。そして、ドアロック制御装置100に紛失鍵の抹消指示を送る（ステップS348）。ステップS346で、バックアップ鍵情報が登録されていないと判別したときには、ステップS348に即座に進む。

【0320】

ドアロック制御装置100では、抹消指示に従って、紛失鍵情報の抹消を実行した後、抹消完了通知を監視制御装置3に送る。そこで、監視制御装置3は、抹消完了通知の受信を待って（ステップS349）、この処理ルーチンを終了する。

【0321】

なお、ドアロック制御装置100における電子鍵情報の認証には本鍵情報のみ

を用いるようにする場合には、バックアップ鍵情報が存在するときには、ステップ S348 では、紛失鍵の情報と共に、本鍵情報に格上げするバックアップ鍵情報を送るようにする。本鍵情報に格上げするバックアップ鍵情報は、抹消完了の後に、監視制御装置 3 から、ドアロック制御装置 100 に送るようにしてもよい。

【0322】

なお、ドアロック制御装置 100 での登録動作は、上述の監視制御装置での鍵登録動作と同様であるので、ここでは省略する。

【0323】

[他の実施形態]

上述の実施形態は、セキュリティ監視システムも含む通信システムの構成であったので、管理サーバ装置 10 が存在しているが、セキュリティ監視システムが存在しない通信システムの構成も可能である。

【0324】

その場合には、監視制御装置 3 で行なえる機能に、バックアップ鍵登録や紛失鍵抹消を用意する。そして、リモートコマンド 50 により、メニューからそれらの機能を選択して、バックアップ鍵登録や、紛失鍵の抹消を行なうようにする。

【0325】

例えば、バックアップ鍵情報の登録は、リモートコマンド 50 により、メニューからバックアップ鍵登録を選択し、監視制御装置 3 に対して、バックアップ鍵情報を登録したい電子鍵装置をかざし、リモートコマンド 50 により、登録要求者の入力を行ない、登録実行を選択することにより、行なうことができる。

【0326】

鍵情報の抹消も同様にして、監視制御装置 3 において行なうことができる。この例の場合にも、監視制御装置 3 からドアロック制御装置 100 に鍵情報を転送したり、抹消指示をしたりするのは、上述の場合と同様である。

【0327】

また、ドアの施錠および開錠のみを目的とするドアロック制御システムとして考えた場合には、監視制御装置 3 は不要である。その場合には、ドアロック制御

装置 100 に対して、バックアップ鍵情報の登録を行ったり、紛失鍵情報の抹消を行ったりすることができる構成とすればよい。

【0328】

上述の例では、バックアップ鍵情報が登録されていても、本鍵情報のみを電子鍵装置からの識別情報の受信時の認証用としたが、家族情報メモリ 120 または 205 に登録されているバックアップ鍵情報をも含む全てを認証用として、常時、用いるようにしても勿論よい。

【0329】

その場合には、鍵紛失による抹消は、当該鍵情報の抹消を行なうだけでよく、上述の例のように、バックアップ鍵を本鍵情報に格上げするようにする処理は不要となる。

【0330】

なお、上述の実施形態では、本鍵情報は、予め管理サーバ装置にドアロック装置の設置会社や販売会社などにより、登録しておくようにしたが、本鍵情報もバックアップ情報と同様にして、上述のようにして後から登録することができるようにしてもよい。

【0331】

また、上述の実施形態では、パーソナルコンピュータを用いてバックアップ鍵の登録を行なうようにしたが、監視制御装置 3 から管理サーバ装置 10 にアクセスすることにより、行なうこともできる。その場合には、監視制御装置 3 が備える電子鍵リード／ライト部 36 を利用することができるので、電子鍵リード／ライト装置を別個に用意する必要はない。

【0332】

また、パーソナルコンピュータの代わりに、電子鍵リード／ライト装置に接続される携帯電話端末から、管理サーバ装置のホームページにアクセスして、バックアップ鍵登録を行なうようにすることもできる。

【0333】

また、上述の実施形態では、電子鍵情報の紛失届による抹消は、本鍵情報について説明したが、紛失届の際に、本鍵情報の紛失届か、バックアップ鍵情報の紛

失届かの指定をすることにより、バックアップ鍵情報の紛失届およびそれに基づくバックアップ鍵情報の抹消処理をすることもできる。

【0334】

また、ICチップのメモリには、予め一元管理された識別情報が記憶されているように説明したが、後から、一元管理されている識別情報が書き込まれるようにされてもよいことは言うまでもない。

【0335】

なお、上述の実施形態では、電子鍵装置を、外側電子鍵リード／ライト部 21ex に対して、ドアの施錠後、所定時間以内にかざした場合に、セキュリティモードをオンにするようにしたが、ドアロック制御装置 100 または監視制御装置 3 では、玄関ドア 1 からの入退出を管理しているので、在宅者が無くなったら、自動的にセキュリティレベル A でセキュリティモードをオンにするようにすることもできる。

【0336】

その場合に、ドアロック制御装置 100 で、在宅者無しを検出したときに、監視制御装置 3 にセキュリティモードオンを要求しても良いし、監視制御装置 3 が、自装置で、在宅者無しを検出したときに、セキュリティモードオンとするようにしても良い。

【0337】

なお、この例では、在宅者が玄関ドア 1 を開錠し、玄関ドア 1 を開けたときには、それまでにセキュリティモードがオンになっていても、一旦、セキュリティモードは、オフとされるものとしたが、セキュリティモードがオンになっているときに外出者があった場合には、外出者を電子鍵装置との通信により取得される識別情報により認識して、監視制御装置 3 が、帰宅者があった場合と全く同様に、在宅状況の変化に対応して自動的にセキュリティレベルを変更するようにすることもできる。

【0338】

なお、以上の実施形態の説明では、鍵情報としての識別情報の認証は、ドアロック装置で行なうようにしたが、ドアロック装置 2 は、監視制御装置 3 に、ある

いは監視制御装置 3 を介して管理サーバ装置 10 に鍵情報を送り、監視制御装置 3 あるいは管理サーバ装置 10 で、認証作業を行ない、その認証結果を、ドアロック装置 2 に返す（管理サーバ装置 10 の場合には監視制御装置 3 を介して返す）ようにしても良い。その場合には、監視制御装置 3 からドアロック制御装置 100 への鍵情報の転送や抹消指示を送る必要はない。

【0339】

また、開錠者、施錠者の識別情報も監視制御装置 3 ではなく、管理サーバ装置 10 に送り、管理サーバ装置 10 により、セキュリティ管理をするようにしてもよい。

【0340】

また、以上の説明では、外出者か帰宅者かは、ドアロック制御装置 100 で判別するようにしたが、監視制御装置 3 においても、ドアロック制御装置 100 でのドアロック制御モードの設定情報を備えているので、ドアロック制御装置 100 は、電子鍵装置 40 が、内側電子鍵リード／ライト部 21 i n または外側電子鍵リード／ライト部 21 e x にかざされて通信が両者の間で行なわれ、識別情報についての認証がとれたときには、その識別情報と、内側電子鍵リード／ライト部 21 i n または外側電子鍵リード／ライト部 21 e x のいずれと通信したかの情報と、開錠か施錠かの情報とを、監視制御装置 3 に送り、監視制御装置 3 が、外出か帰宅かを判別するようにすることもできる。

【0341】

また、電子鍵装置は、上述の実施形態のような非接触形式で電子鍵情報の通信を行なうのものに限られるものではなく、接触形式で電子鍵情報の通信を行なうものであっても勿論よい。

【0342】

【発明の効果】

以上説明したように、この発明によれば、同一のものが存在しないように一元管理された識別情報を電子鍵情報として用いることができるようにしたので、ドアの施錠、開錠に関するセキュリティを向上させることができる。

【0343】

また、前記識別情報は、同一のものが存在しないユニークなものであるので、これを使用者個人に対応させて管理することができる。その場合には、ドアからの入退出を個人レベルで管理することができ、在宅状況に応じたセキュリティ管理ができるなどの効果がある。

【図面の簡単な説明】

【図 1】

この発明の実施形態の識別情報の概要を説明するための図である。

【図 2】

この発明の実施形態で用いる識別情報の一例を示す図である。

【図 3】

ドアロックシステムの実施形態を含むセキュリティシステムの概要を説明するための図である。

【図 4】

ドアロックシステムの実施形態の要部を説明するための図である。

【図 5】

実施形態のドアロック装置の構成例を示す図である。

【図 6】

この発明の実施形態に用いる電子鍵装置の一例を示す図である。

【図 7】

図 6 の電氣的構成例を示す図である。

【図 8】

セキュリティシステムに用いる監視制御装置の例を示す図である。

【図 9】

図 5 の監視制御装置の構成例を示すブロック図である。

【図 10】

個人プロフィール情報の一例を示す図である。

【図 11】

セキュリティモードの内容を説明するための図である。

【図 12】

セキュリティモードの内容を説明するための図である。

【図 13】

管理サーバ装置の構成例を示すブロック図である。

【図 14】

図 5 の監視制御装置の伝言記録および再生機能を説明するためのフローチャートである。

【図 15】

ドアロック制御モードの設定動作を説明するためのフローチャートである。

【図 16】

ドアロック制御モードの設定動作を説明するためのフローチャートである。

【図 17】

ドアロック制御モードの一つの例であるオートロックモードでのドアロック制御動作を説明するためのフローチャートの一部である。

【図 18】

ドアロック制御モードの一つの例であるオートロックモードでのドアロック制御動作を説明するためのフローチャートの一部である。

【図 19】

ドアロック制御モードの一つの例であるオートロックモードでのドアロック制御動作を説明するためのフローチャートの一部である。

【図 20】

ドアロック制御モードの一つの例であるオートロックモードでのドアロック制御動作を説明するためのフローチャートの一部である。

【図 21】

ドアロック制御モードの一つの例であるオートロックモードでのドアロック制御動作を説明するためのフローチャートの一部である。

【図 22】

ドアロック制御モードの一つの例であるオートロックモードでのドアロック制御動作を説明するためのフローチャートの一部である。

【図 23】

ドアロック制御モードの一つの例である逐次ロックモードでのドアロック制御動作を説明するためのフローチャートの一部である。

【図 2 4】

ドアロック制御モードの一つの例である逐次ロックモードでのドアロック制御動作を説明するためのフローチャートの一部である。

【図 2 5】

ドアロック制御モードの一つの例である逐次ロックモードでのドアロック制御動作を説明するためのフローチャートの一部である。

【図 2 6】

監視制御装置のリモートコマンドからの信号の受信処理動作を説明するためのフローチャートである。

【図 2 7】

監視制御装置におけるセキュリティモードオン時の動作を説明するためのフローチャートの一部である。

【図 2 8】

監視制御装置におけるセキュリティモードオン時の動作を説明するためのフローチャートの一部である。

【図 2 9】

監視制御装置におけるドアロック装置との連携動作を説明するための図である。

【図 3 0】

この発明における実施形態において、本鍵情報の登録を説明するためのフローチャートを示す図である。

【図 3 1】

この発明における実施形態において、本鍵情報の登録を説明するためのシステム構成を示す図である。

【図 3 2】

この発明における実施形態において、バックアップ鍵情報の登録を説明するためのシステム構成を示す図である。

【図 3 3】

この発明における実施形態において、バックアップ鍵情報の登録を説明するためのフローチャートを示す図である。

【図 3 4】

この発明における実施形態において、バックアップ鍵情報の登録を説明するためのフローチャートを示す図である。

【図 3 5】

この発明における実施形態において、バックアップ鍵情報の登録を説明するためのフローチャートを示す図である。

【図 3 6】

この発明における実施形態において、紛失鍵情報の抹消を行なう場合のシステム構成を説明するための図である。

【図 3 7】

この発明における実施形態において、紛失鍵情報の抹消を行なう場合の手順を説明するための図である。

【図 3 8】

この発明における実施形態において、紛失鍵情報の抹消を説明するためのフローチャートを示す図である。

【図 3 9】

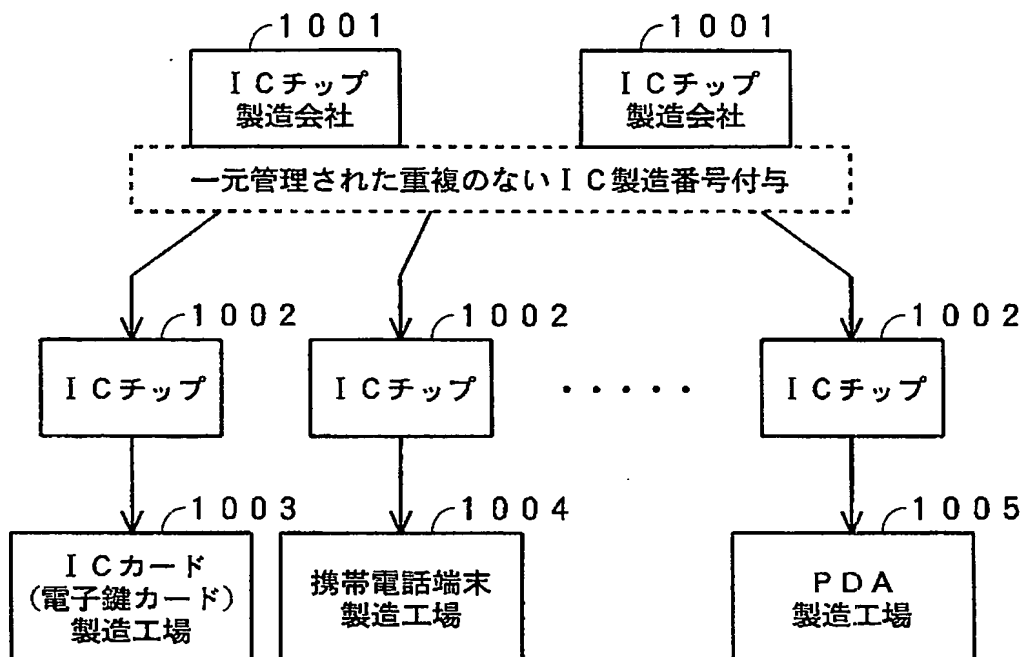
この発明における実施形態において、紛失鍵情報の抹消を説明するためのフローチャートを示す図である。

【符号の説明】

1…玄関ドア、2…ドアロック装置、3…監視制御装置、4…火災センサ、5…ガスセンサ、6 a, 6 b…窓センサ、7…テレビ受像機、8…電話回線、10…管理サーバ装置 100…ドアロック制御装置、21 i n…内側電子鍵リード／ライト部、21 e x…外側電子鍵リード／ライト部、40…電子鍵装置

【書類名】 図面

【図 1】

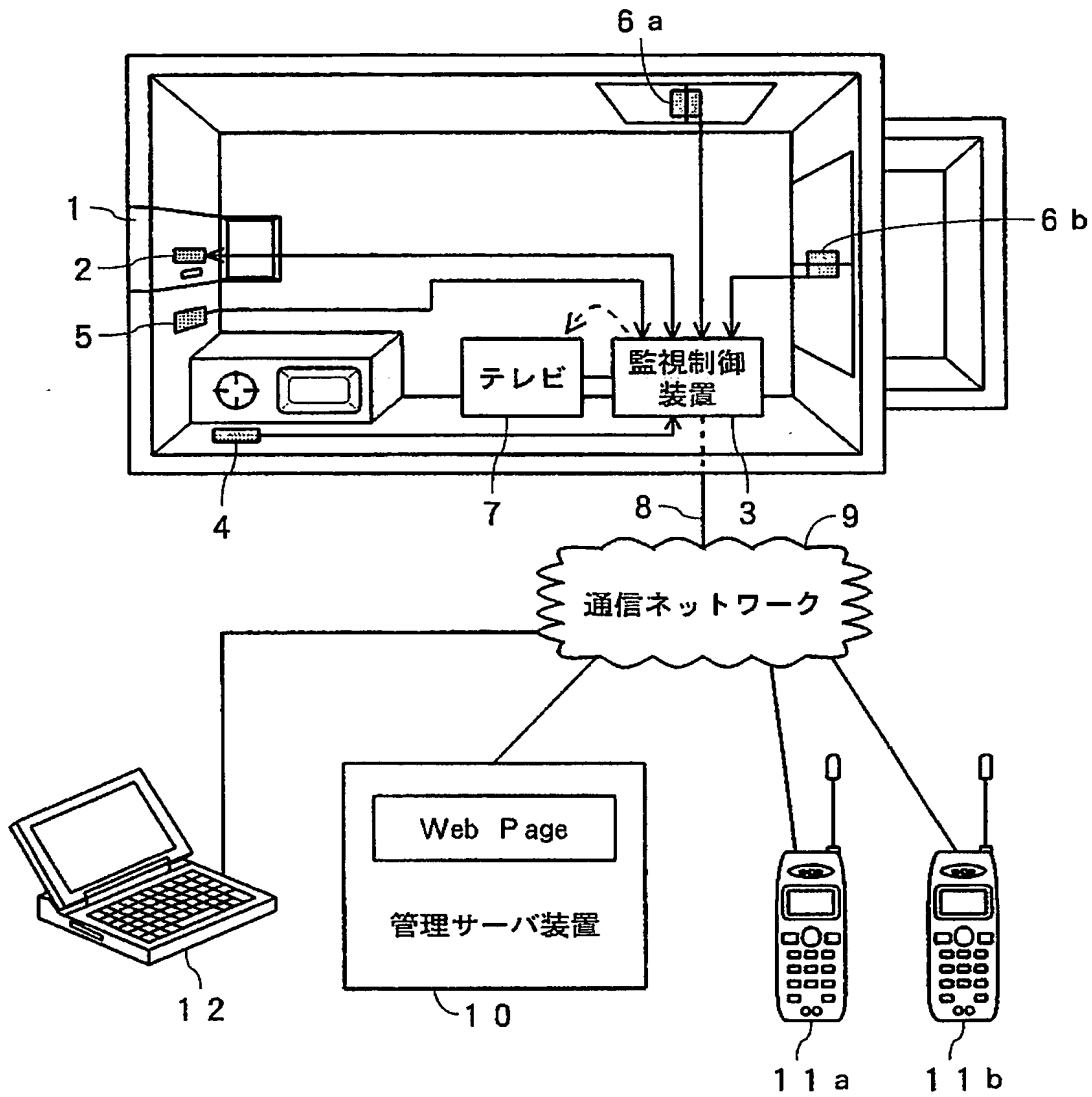


【図 2】

00AKKK0001

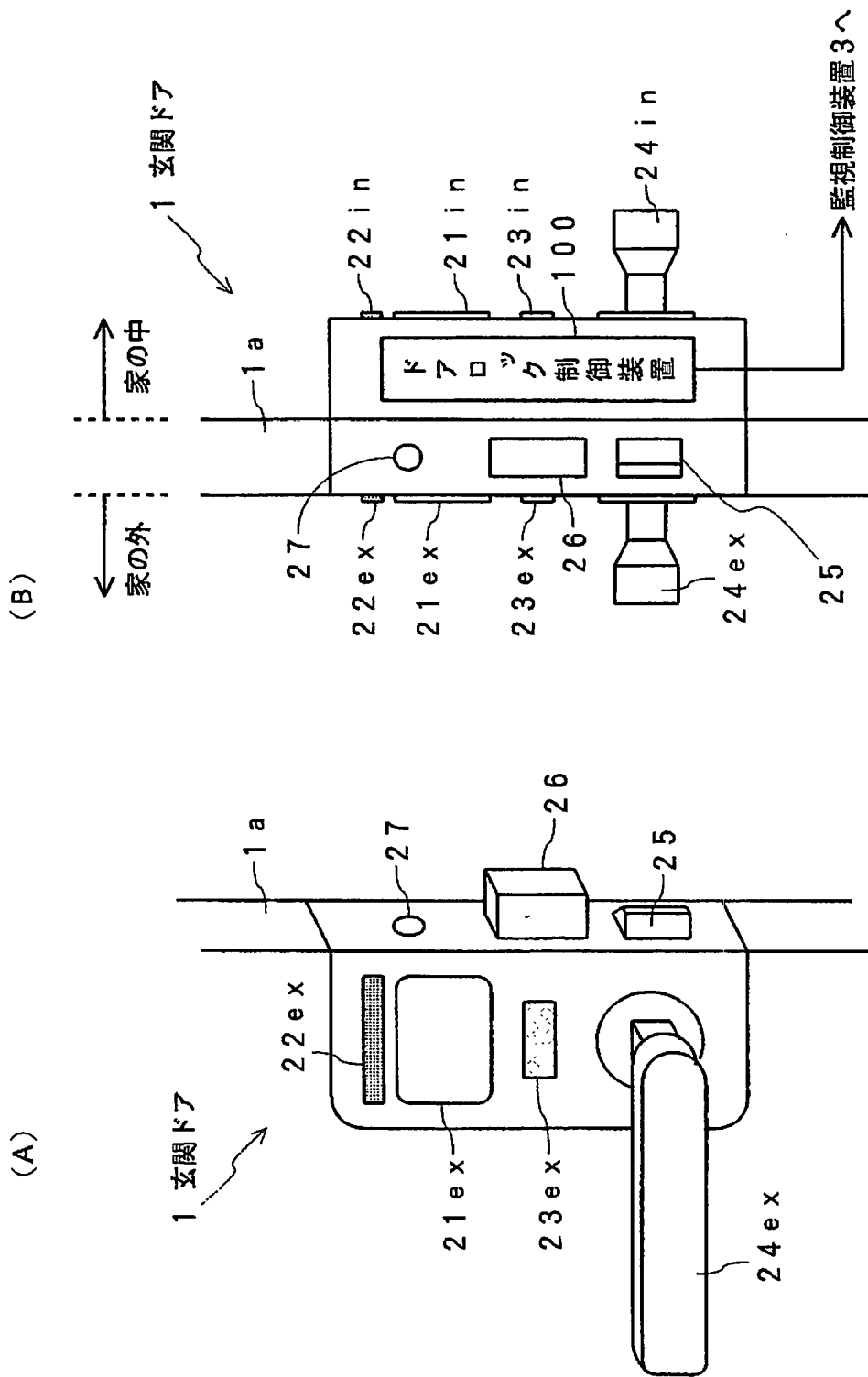
00	A	K	K	K	0	0	0	1
メーカー 番号	カテゴリ コード	シリアル 番号						

【図 3】

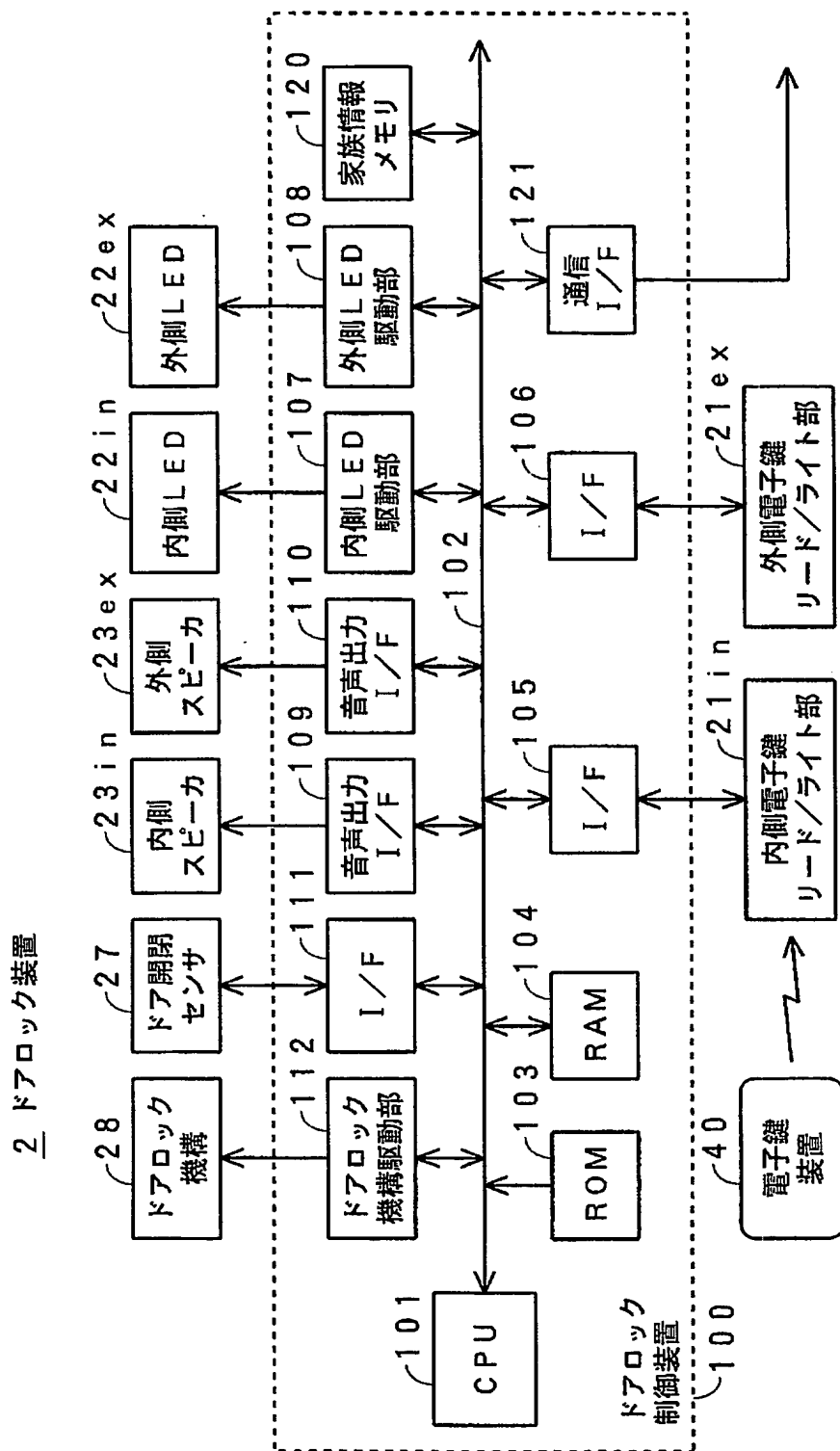


【図4】

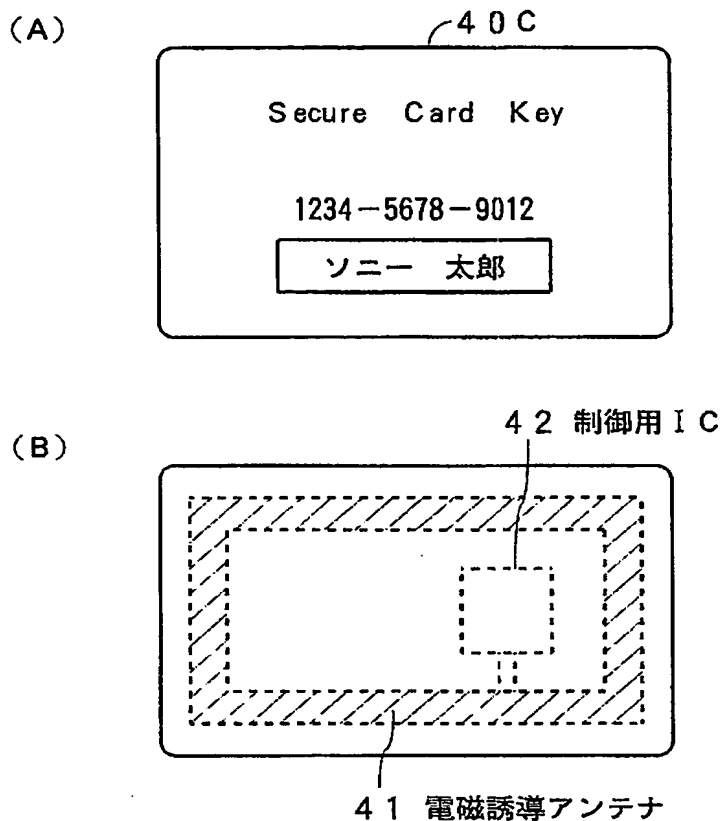
2 ドアロック装置



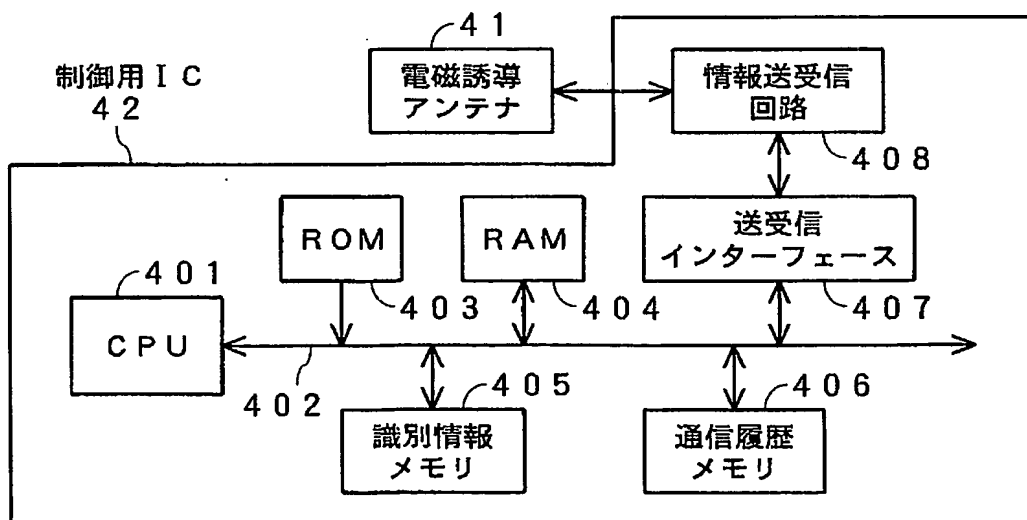
【図 5】



【図 6】

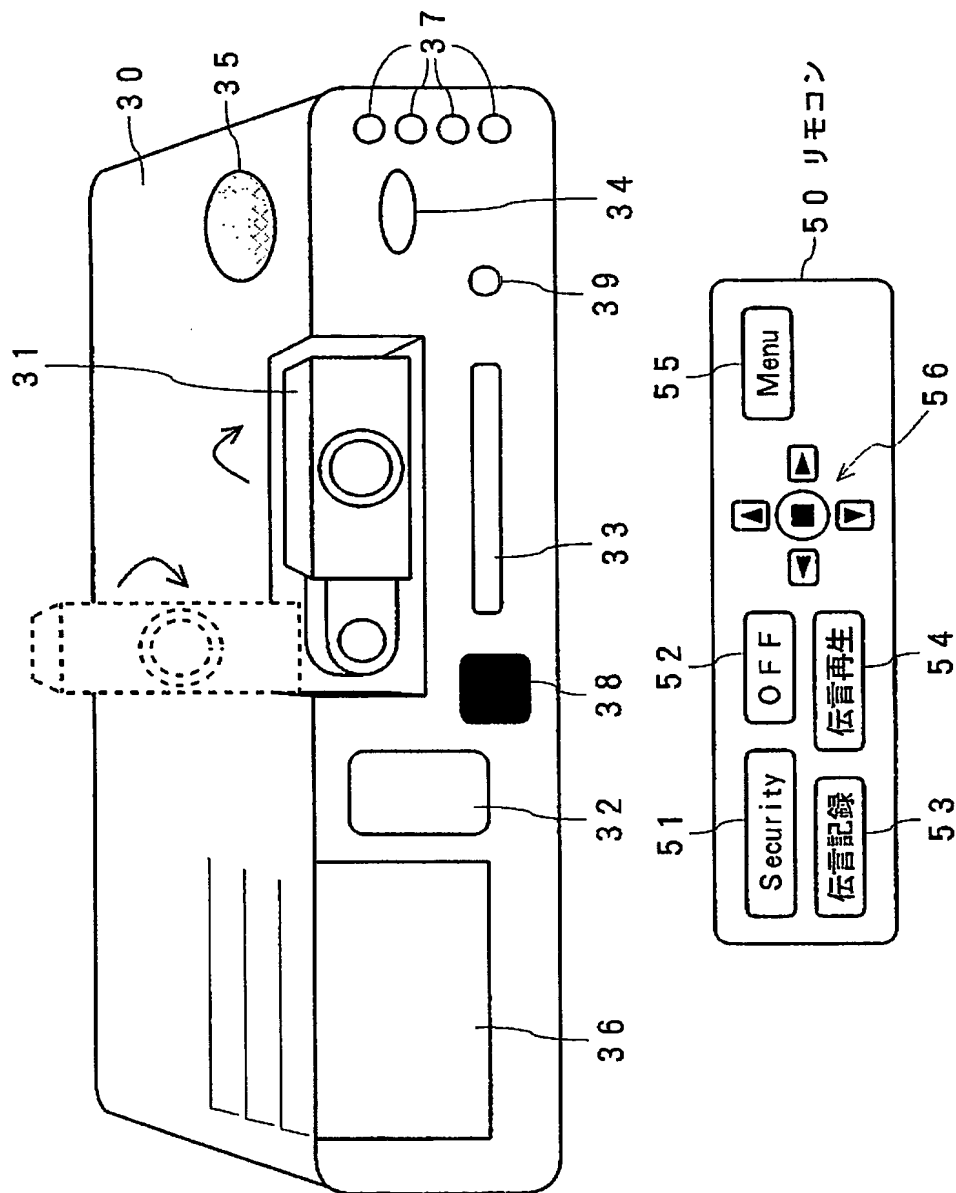


【図 7】

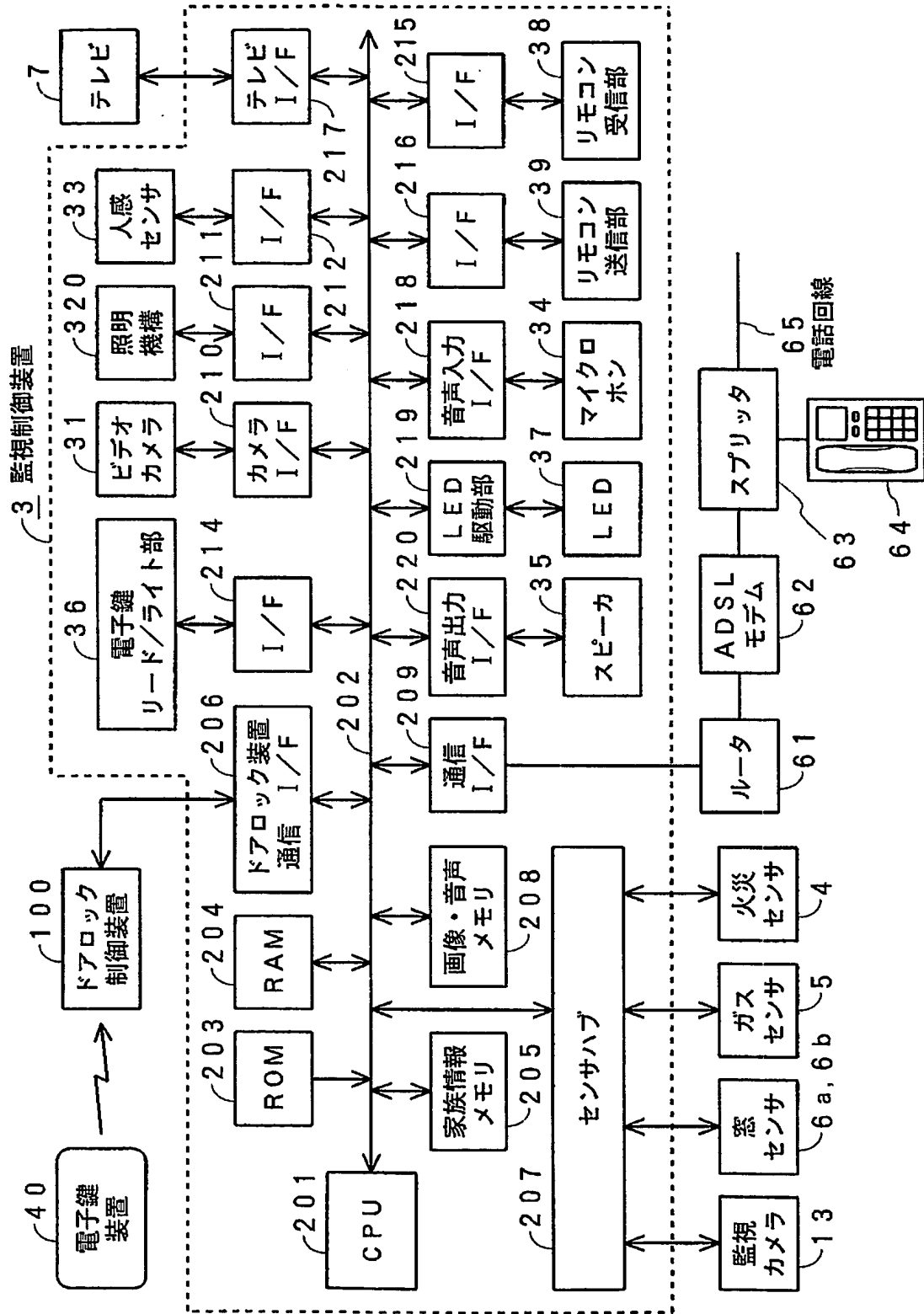


【図 8】

3 監視制御装置



【図9】



【図 10】

個人プロフィール情報

	識別情報 ・ 本鍵情報 ・ バックアップ鍵情報	個人識別情報
	パスワード情報	個人情報
	氏名	
	住所	
	生年月日	
	年齢	
	続柄	
	登録日	
	銀行口座番号	
	電話番号	
	趣味／嗜好情報 ・ 好きなテレビ番組：ドラマ ・ 好きな音楽：ジャズ ・ 好きな映画：S F	
	入退出履歴情報	
	電子鍵登録・紛失履歴情報	

【図 1 1】

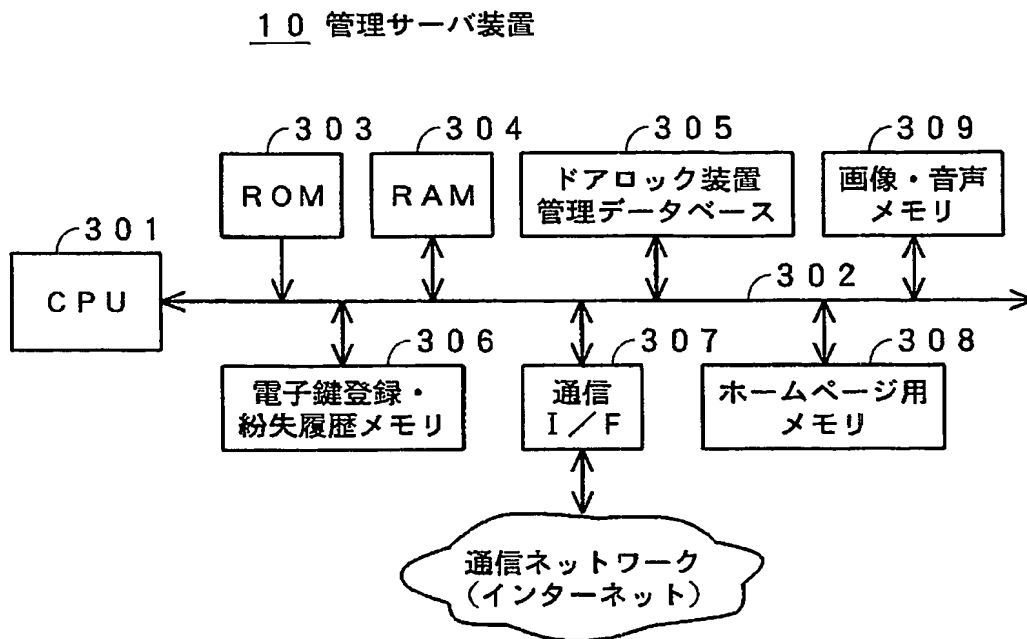
セキュリティレベル	父親	母親	子供
D	○	○	○
D	○	○	×
D	○	×	○
D	○	×	×
C	×	○	○
C	×	○	×
B	×	×	○
A	×	×	×

○：在宅
×：不在

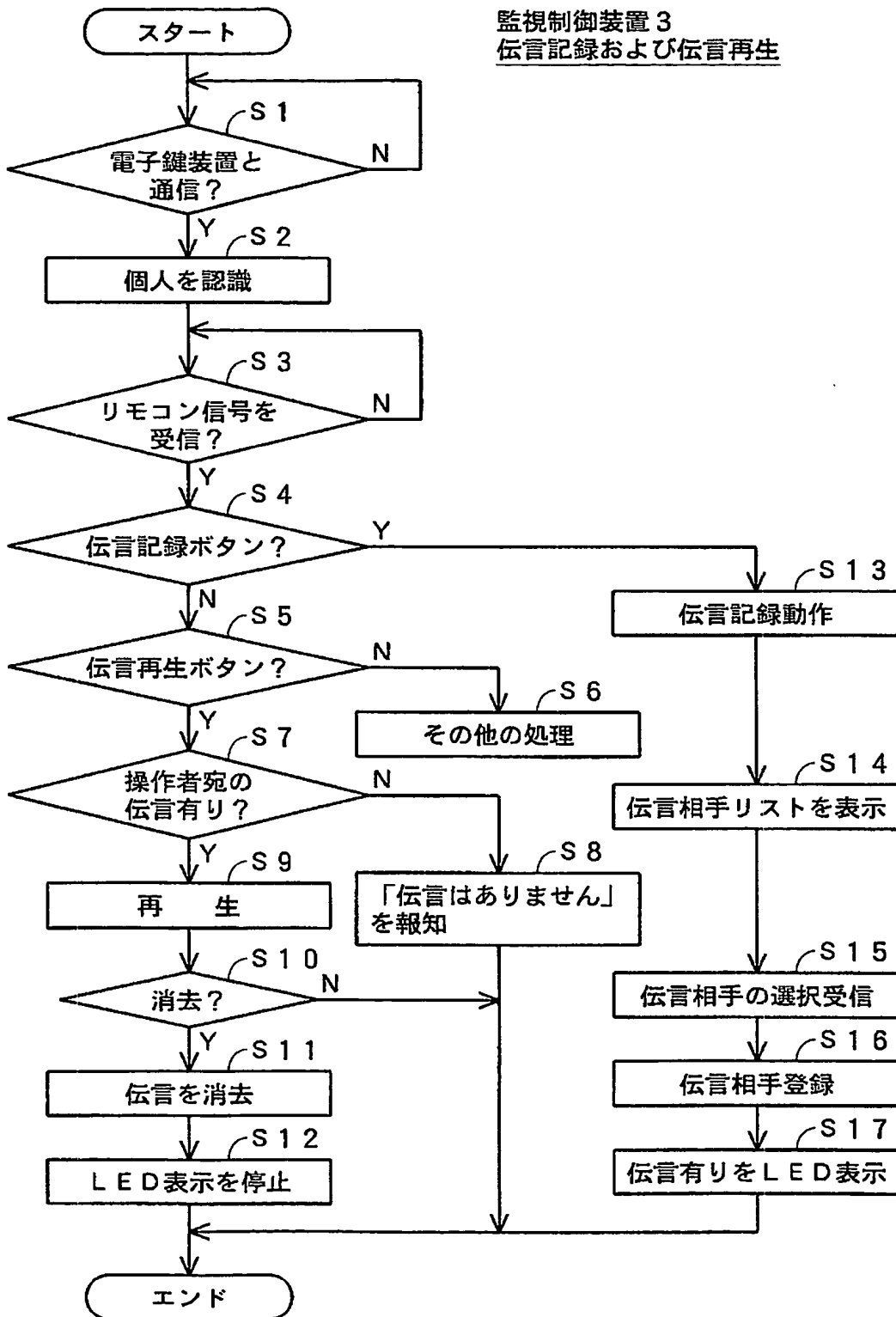
【図 1 2】

セキュリティレベル	窓・ドア監視	火災・ガス監視	カメラ監視
A	○	○	○
B	○	○	×
C	×	○	×
D	×	×	×

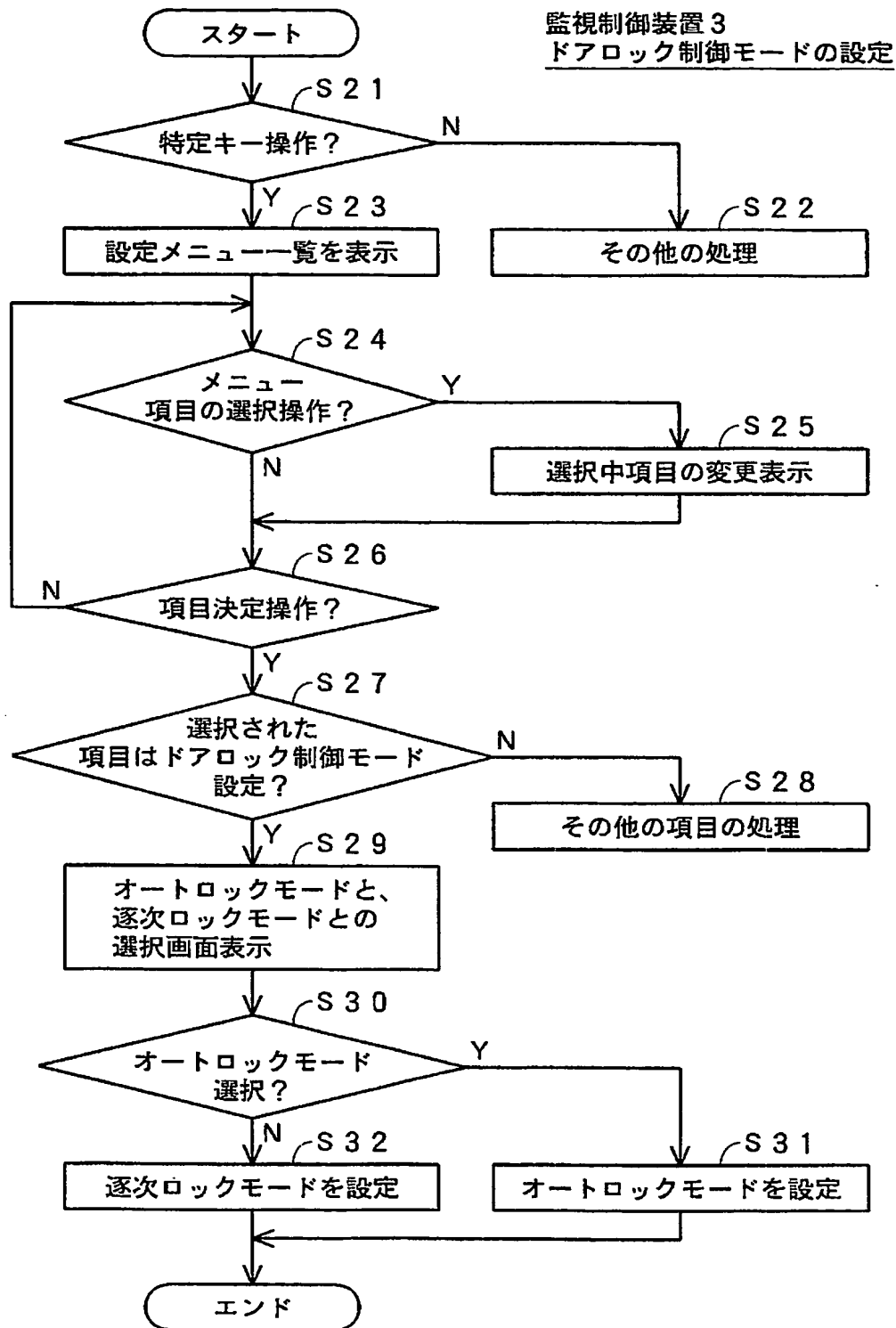
【図 13】



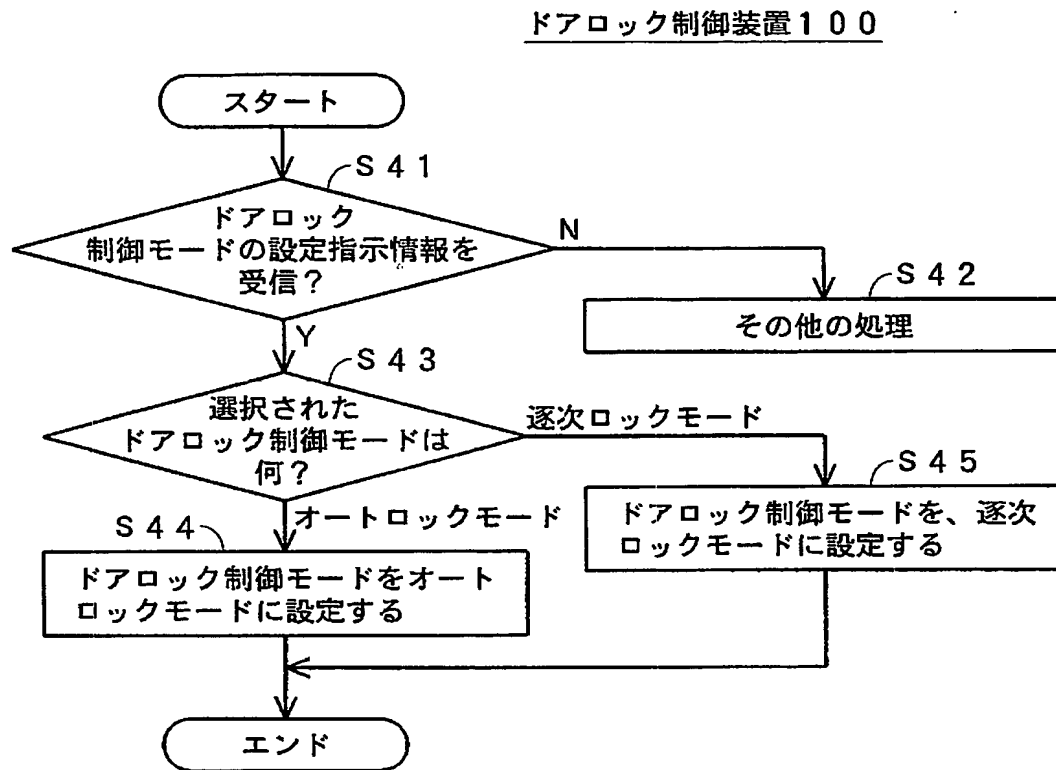
【図 14】



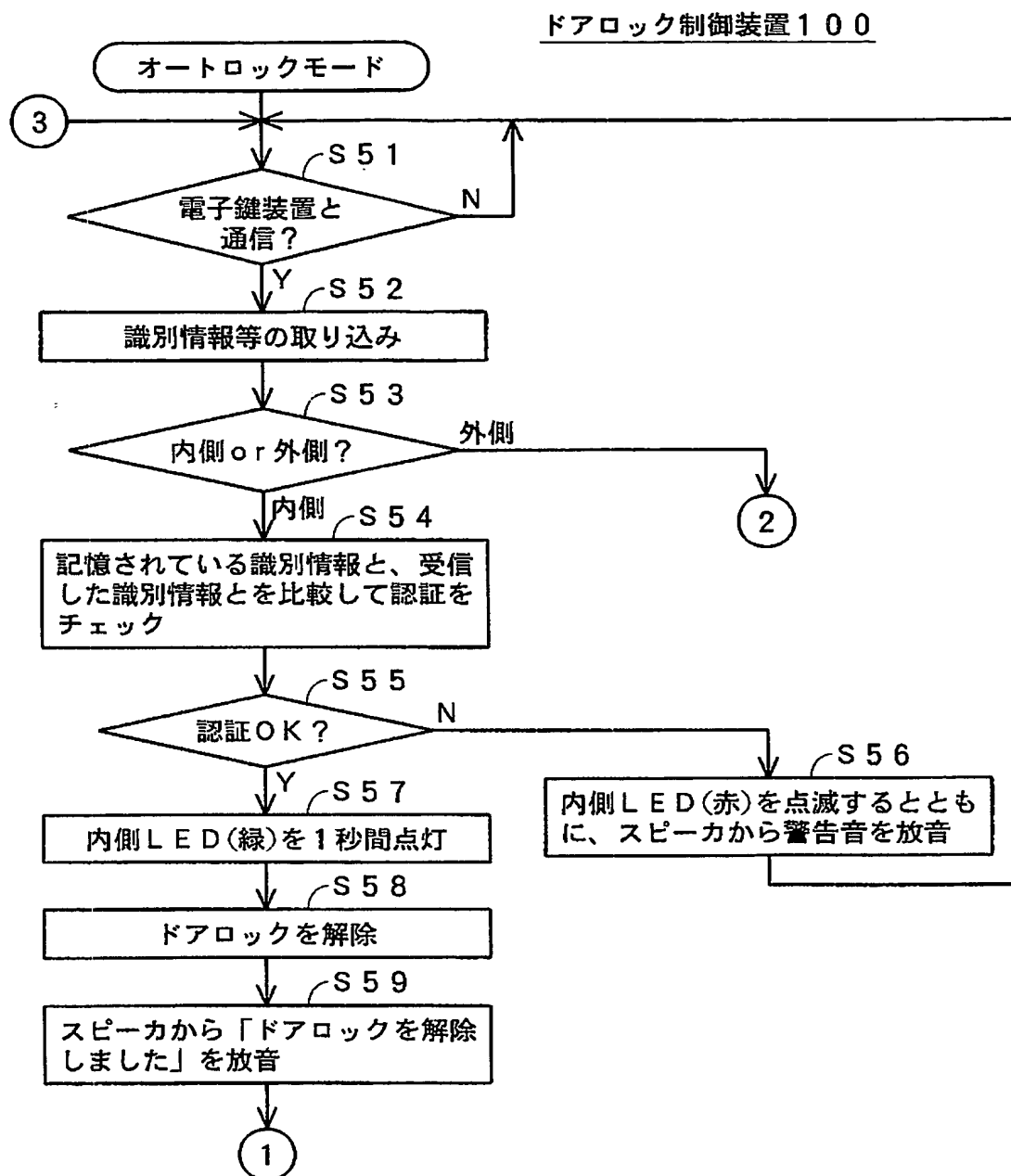
【図 15】



【図16】

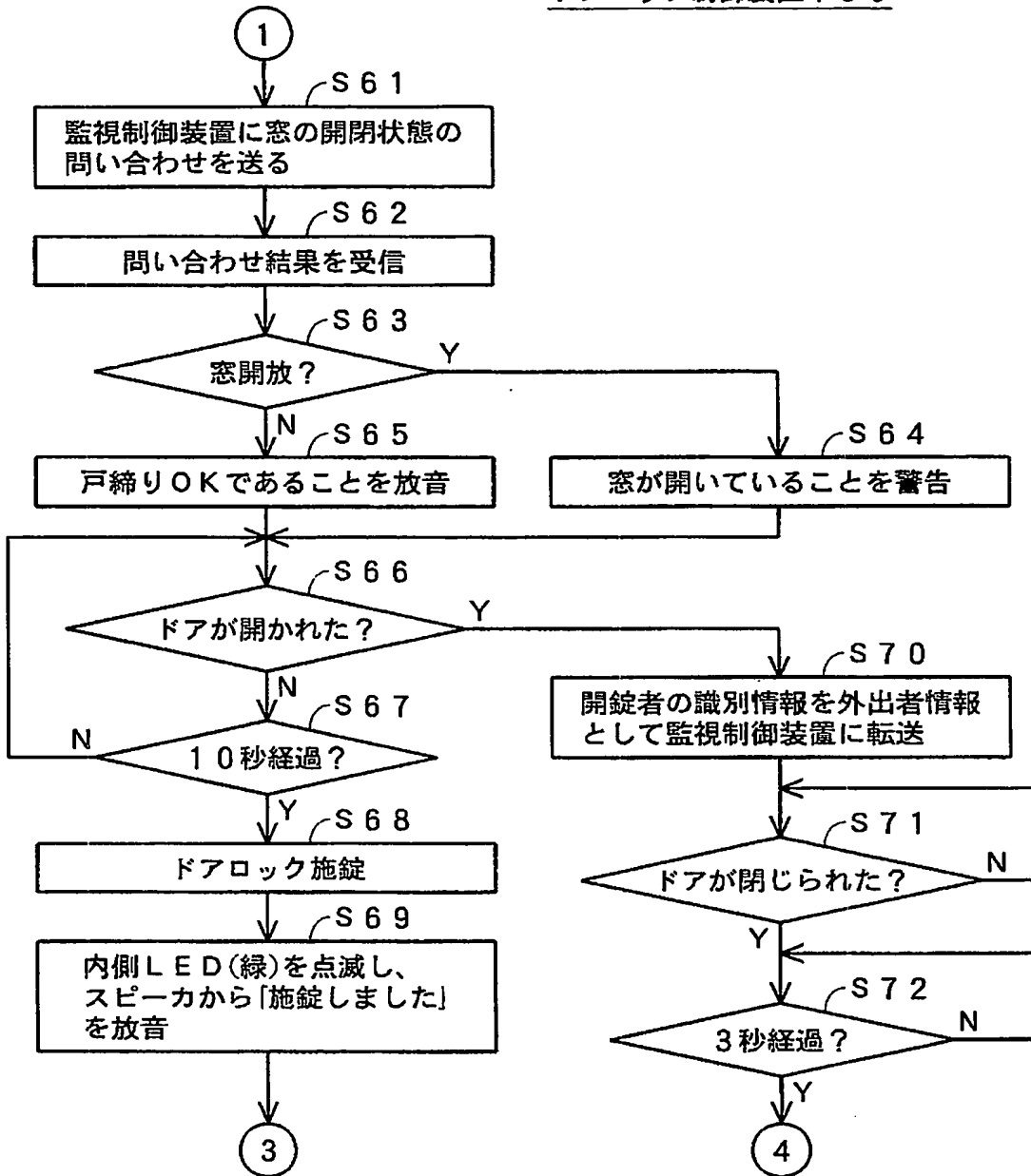


【図 17】



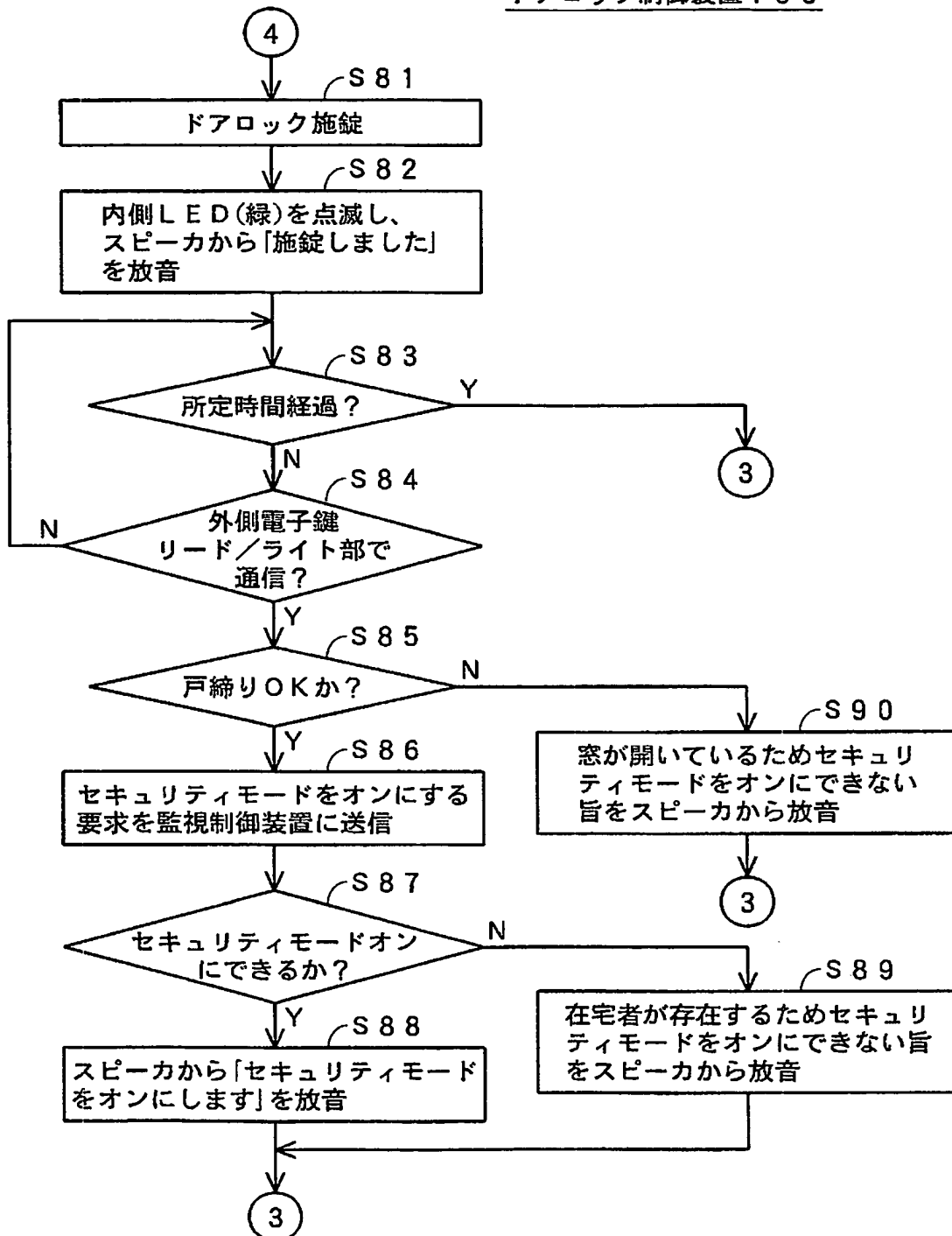
【図 18】

ドアロック制御装置 100

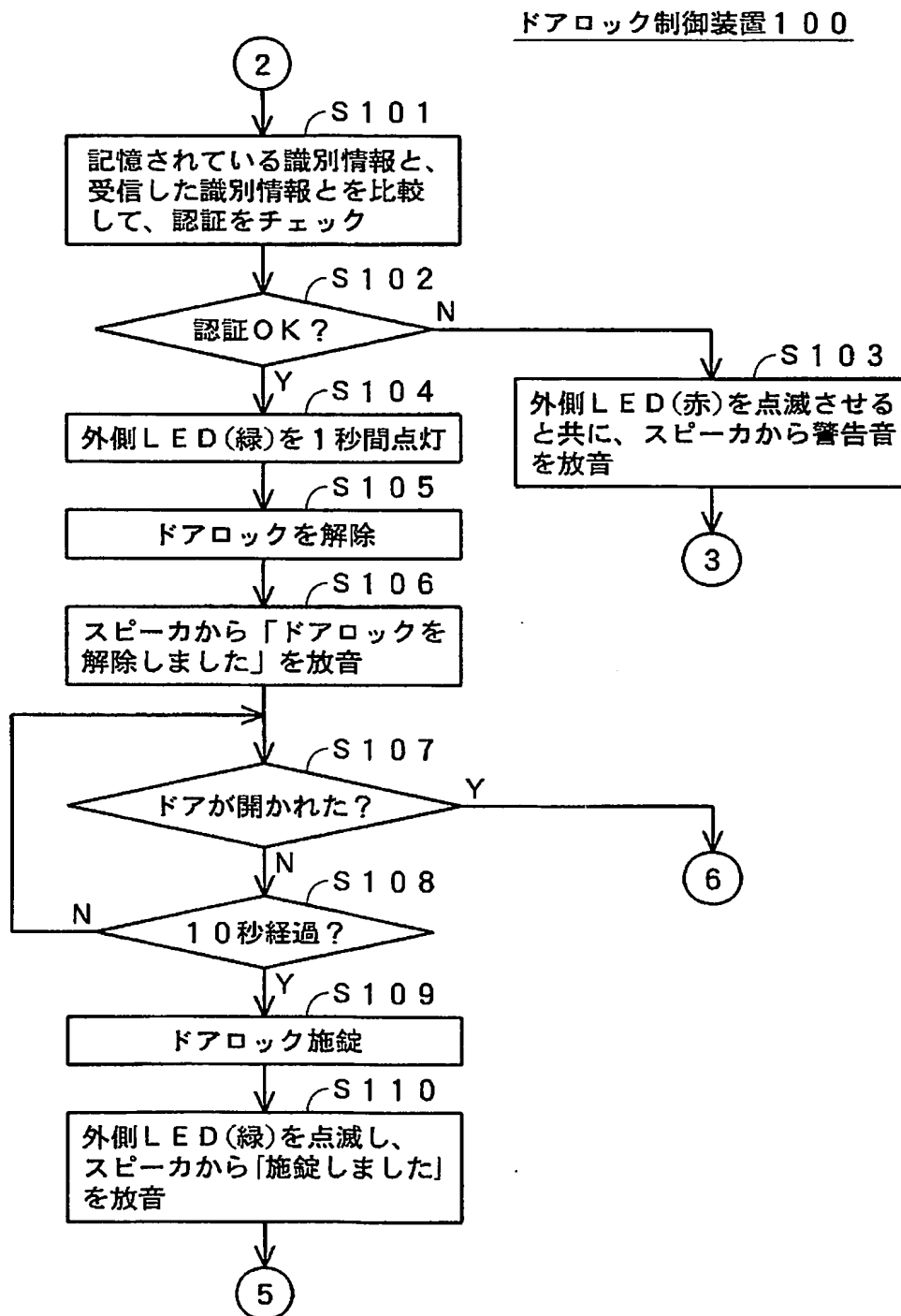


【図 19】

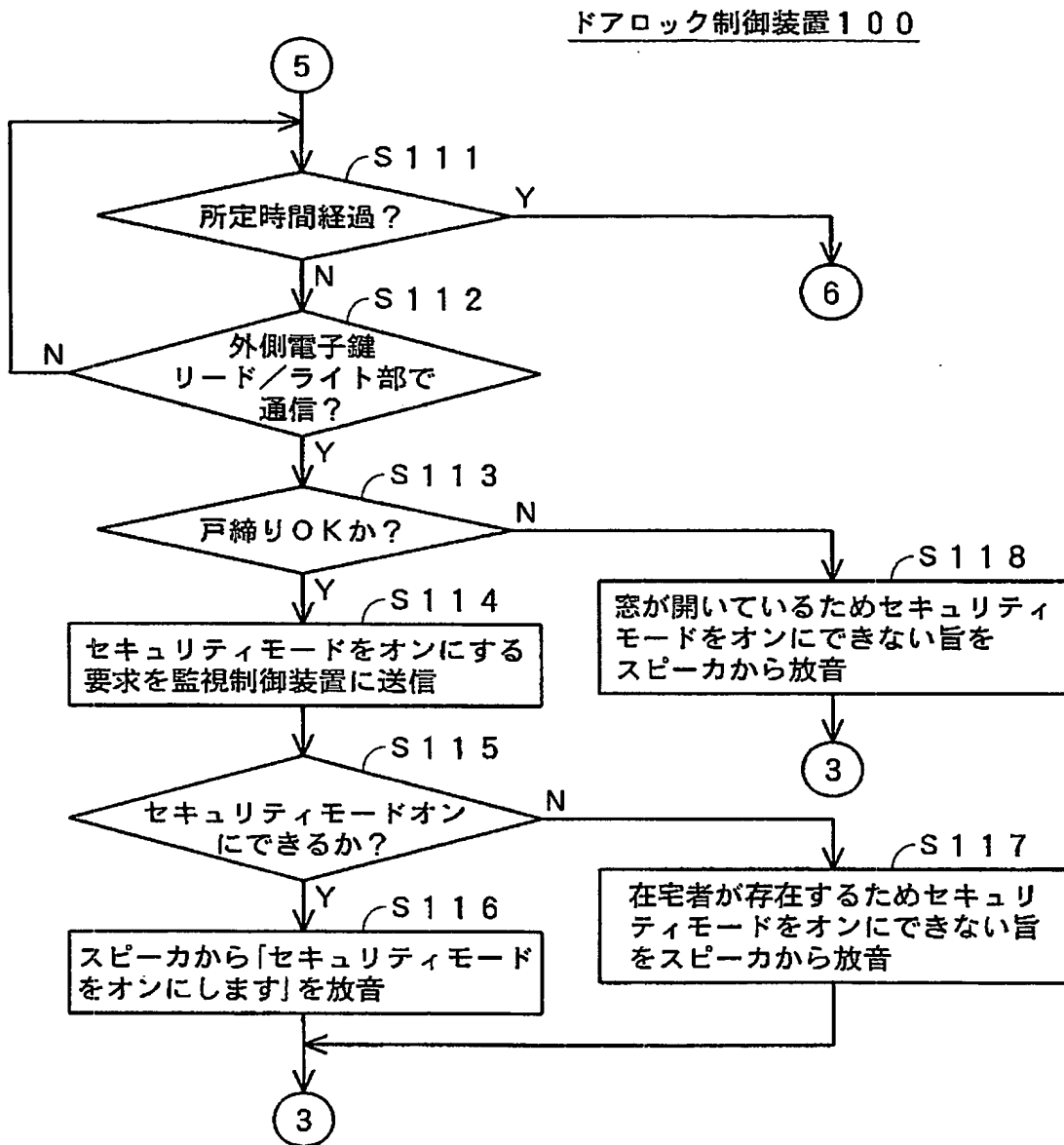
ドアロック制御装置 100



【図 20】

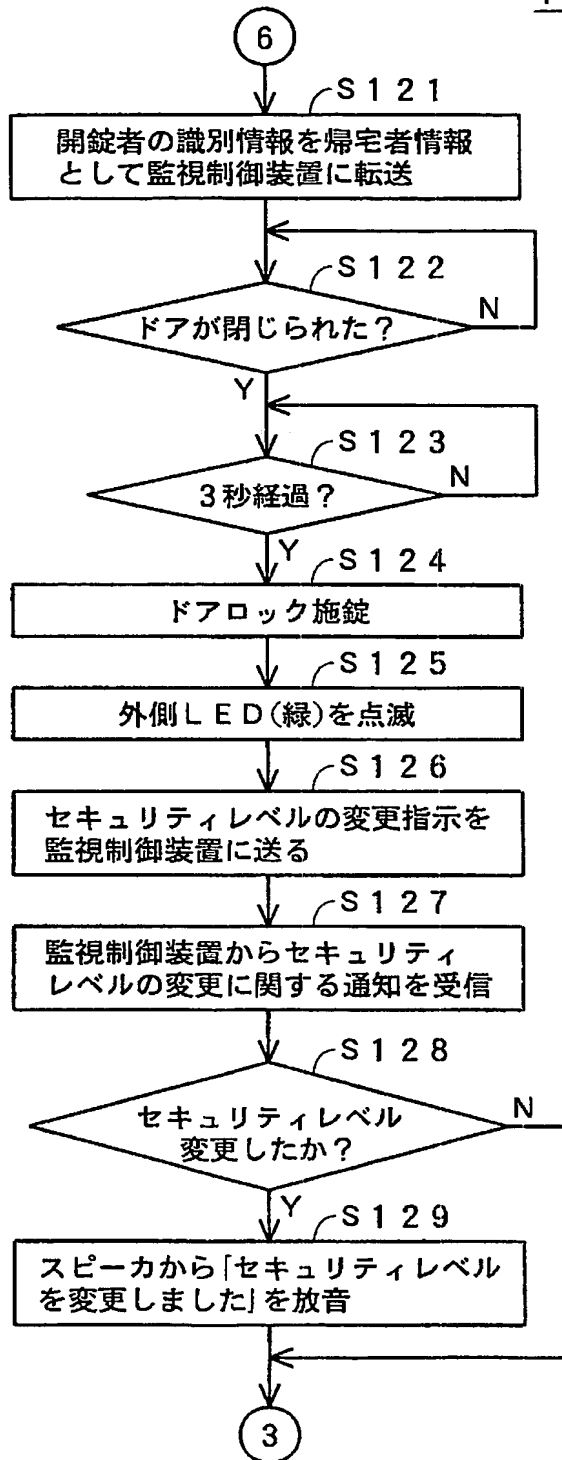


【図 21】

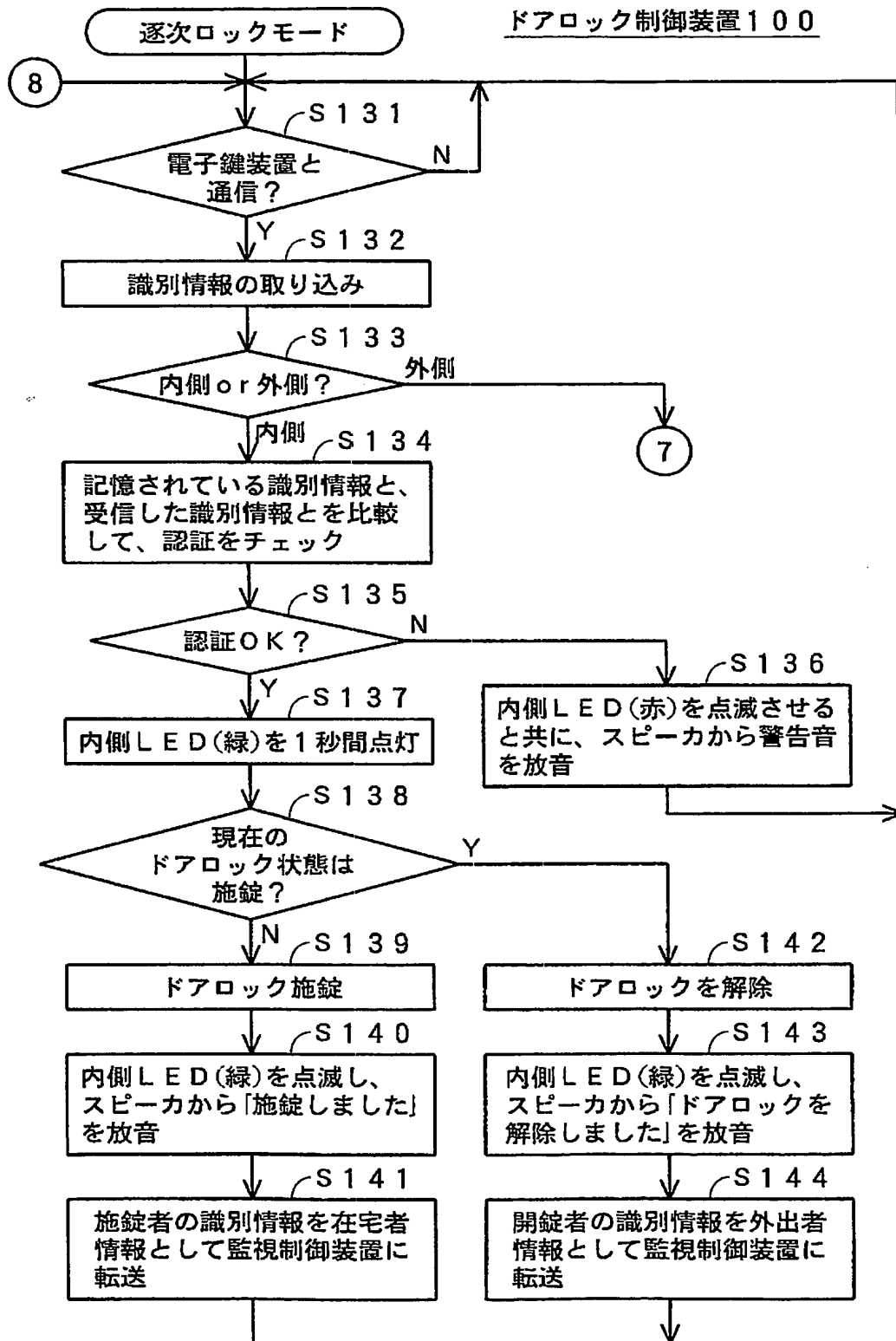


【図 22】

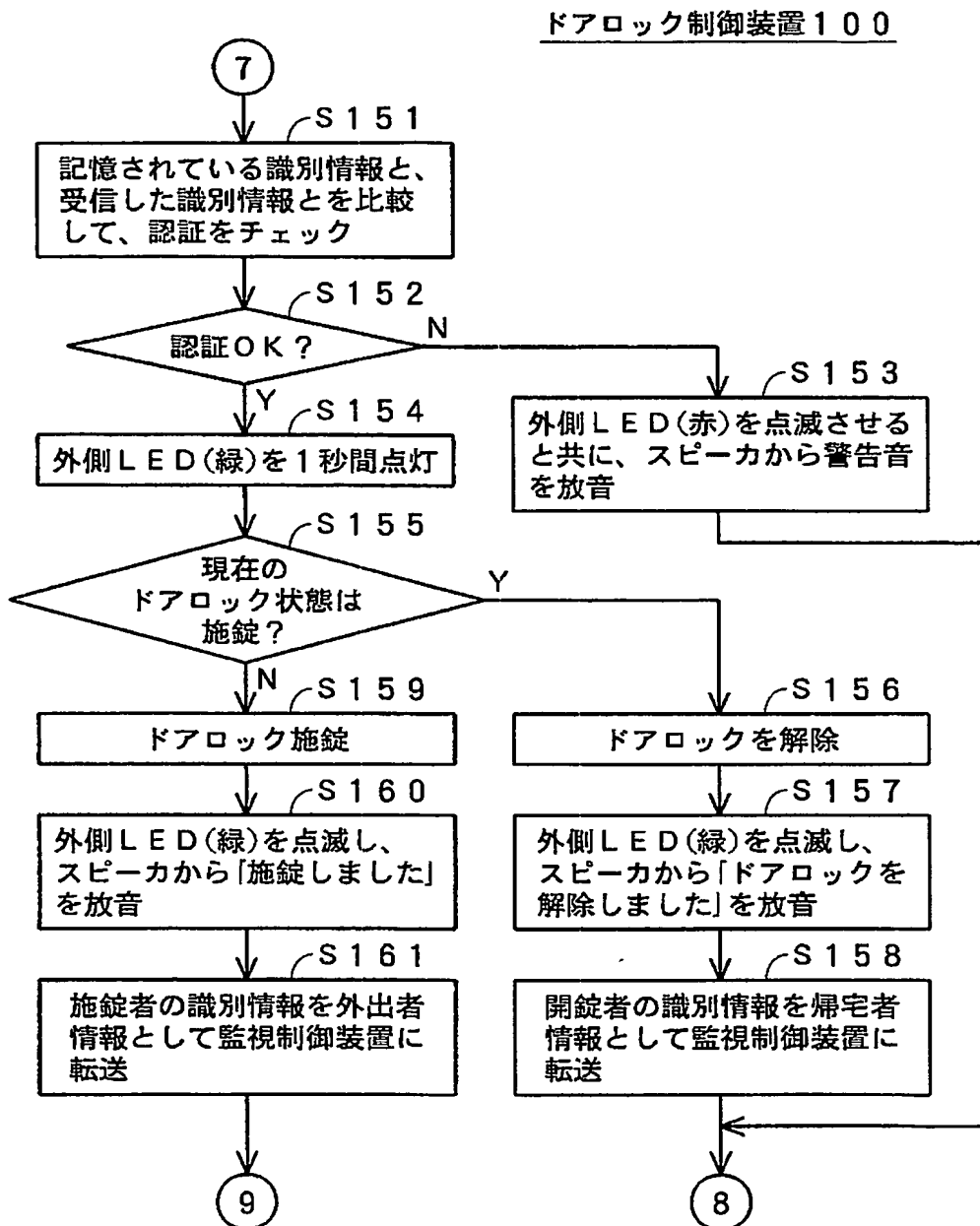
ドアロック制御装置 100



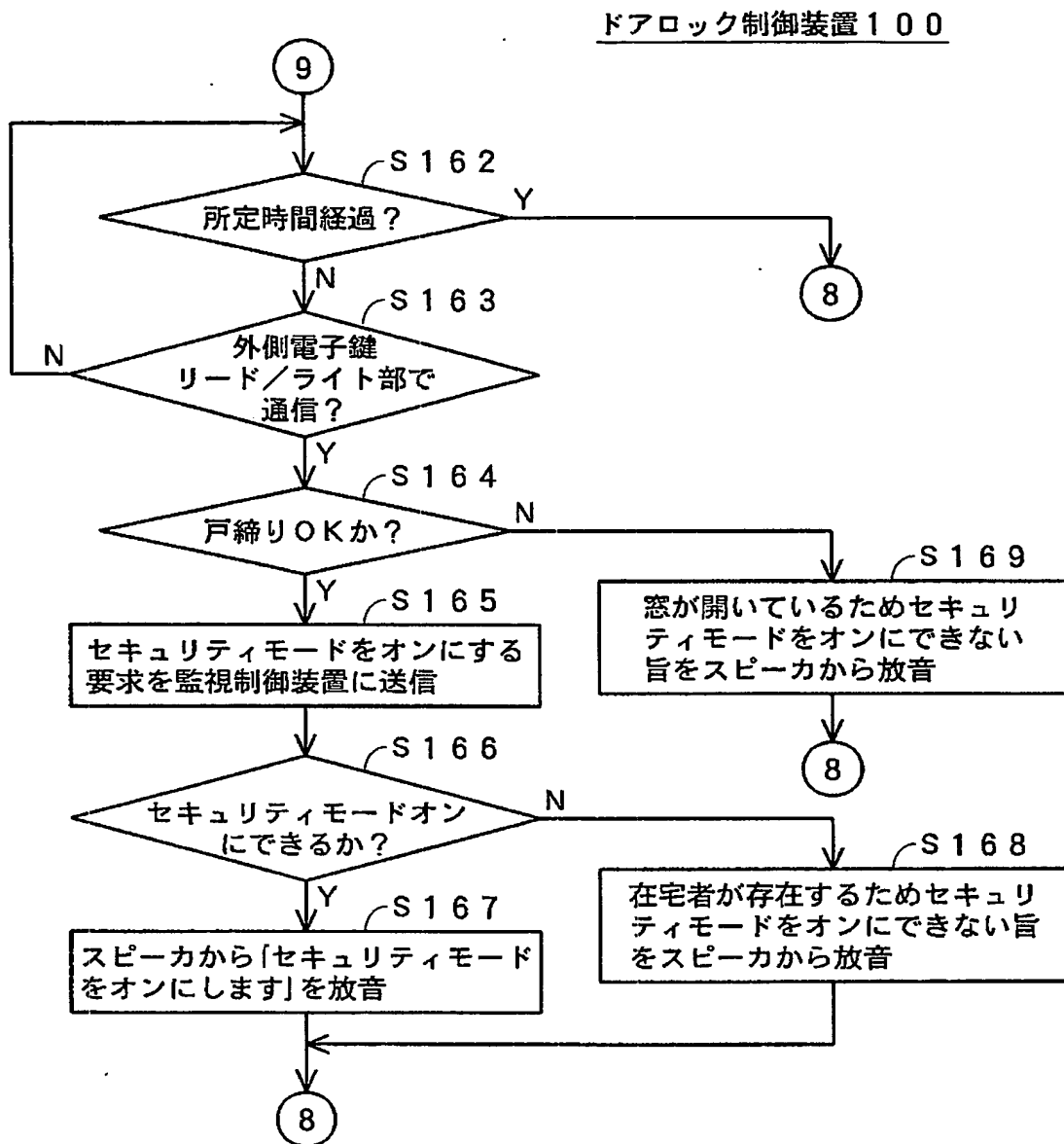
【図 23】



【図 24】

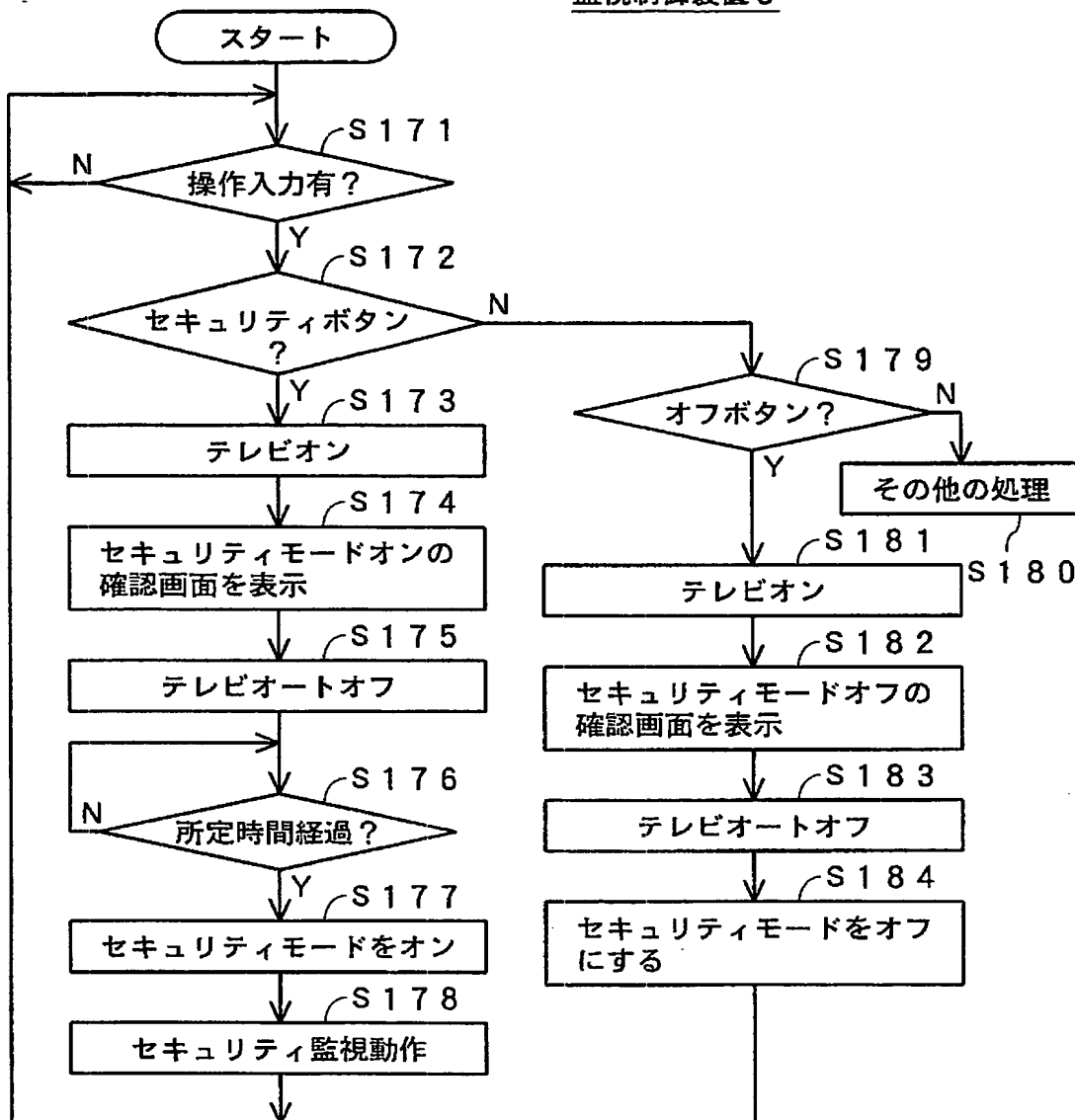


【図 25】

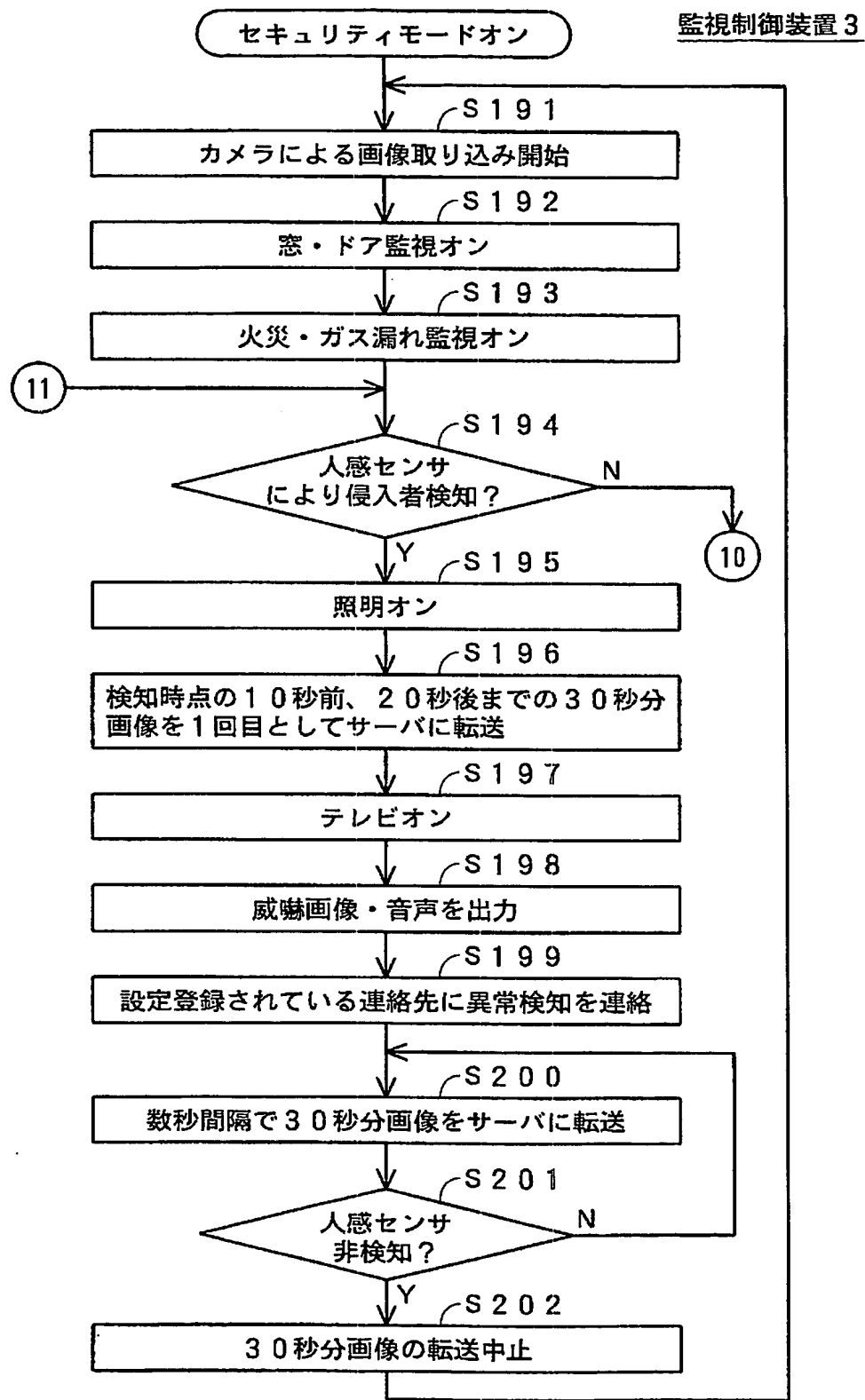


【図 26】

監視制御装置 3

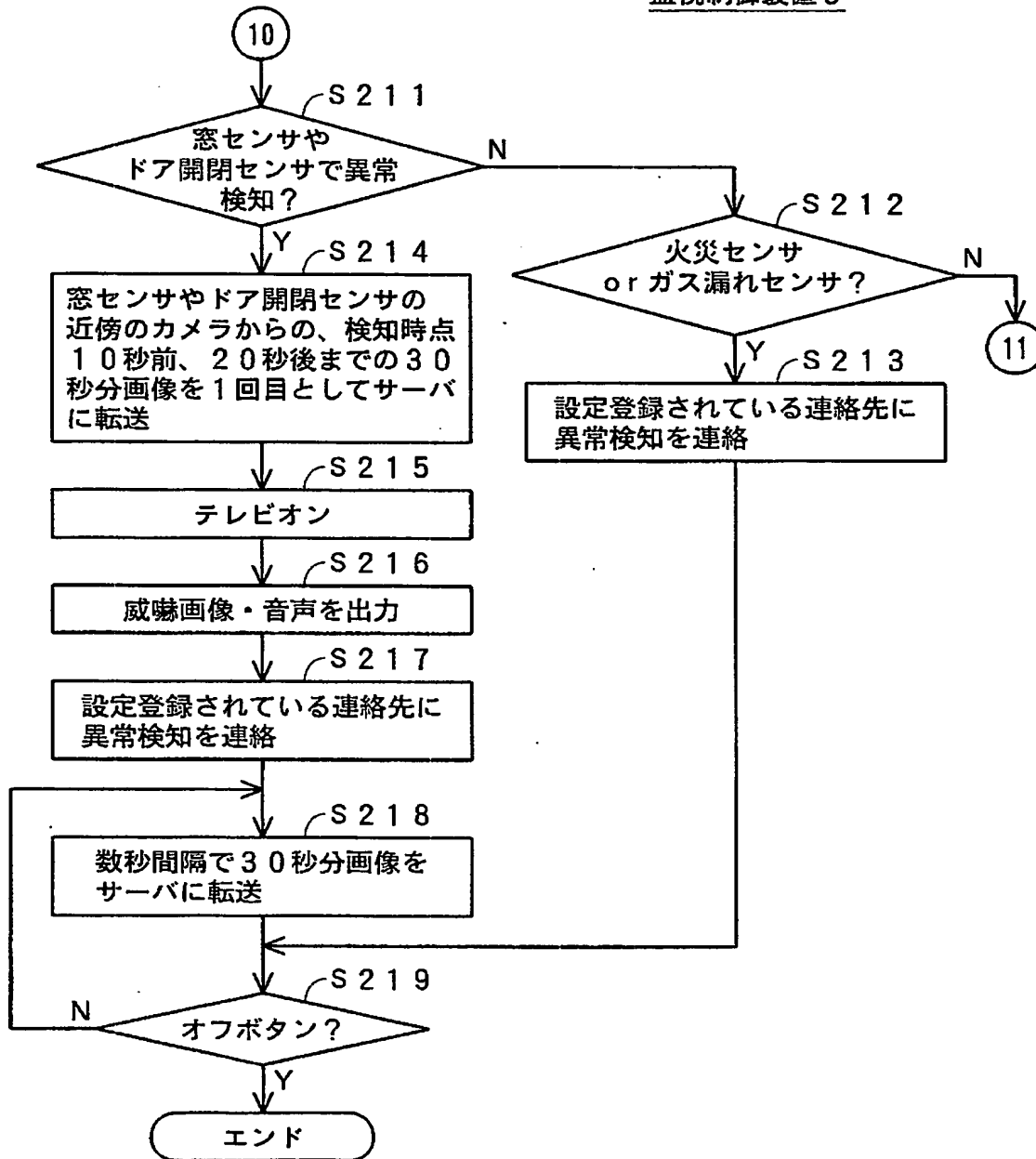


【図 27】

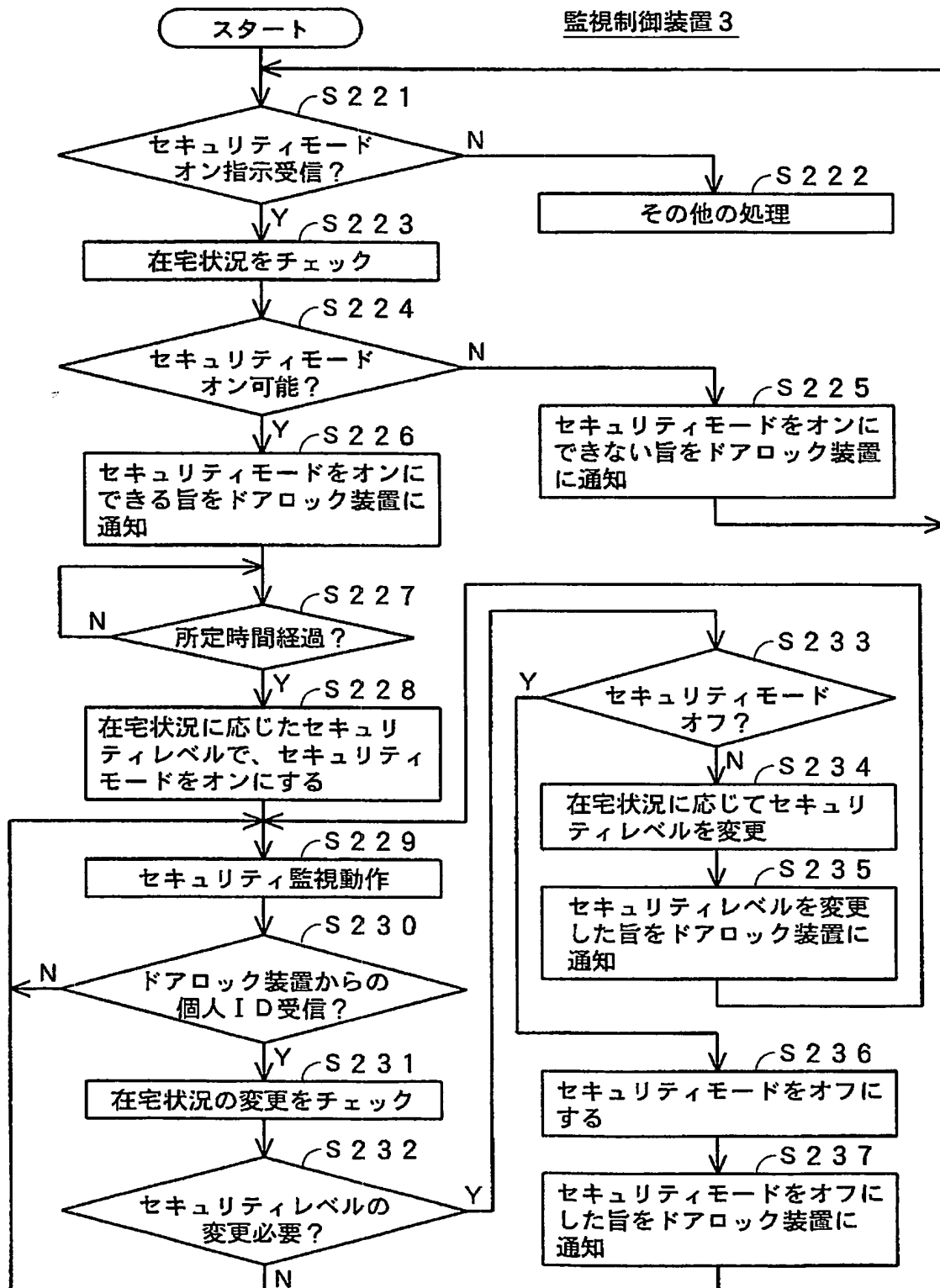


【図 28】

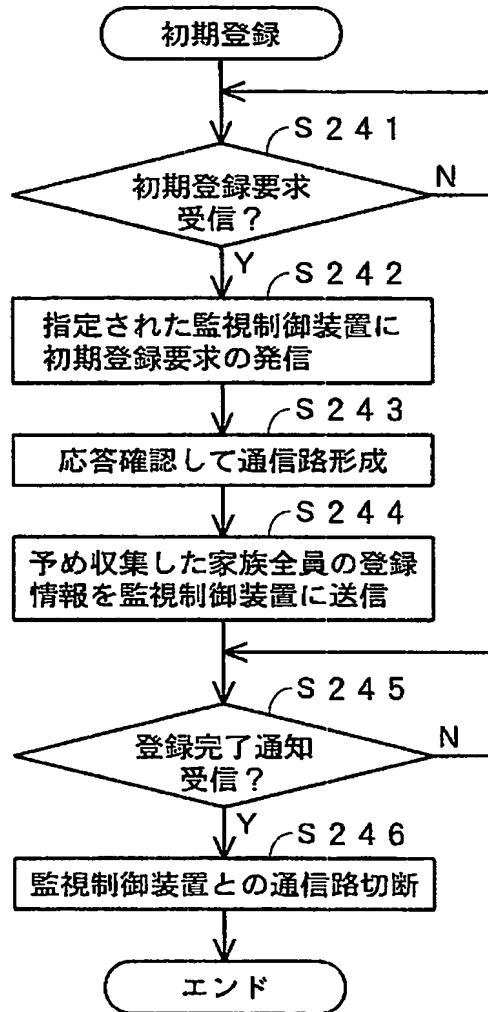
監視制御装置 3



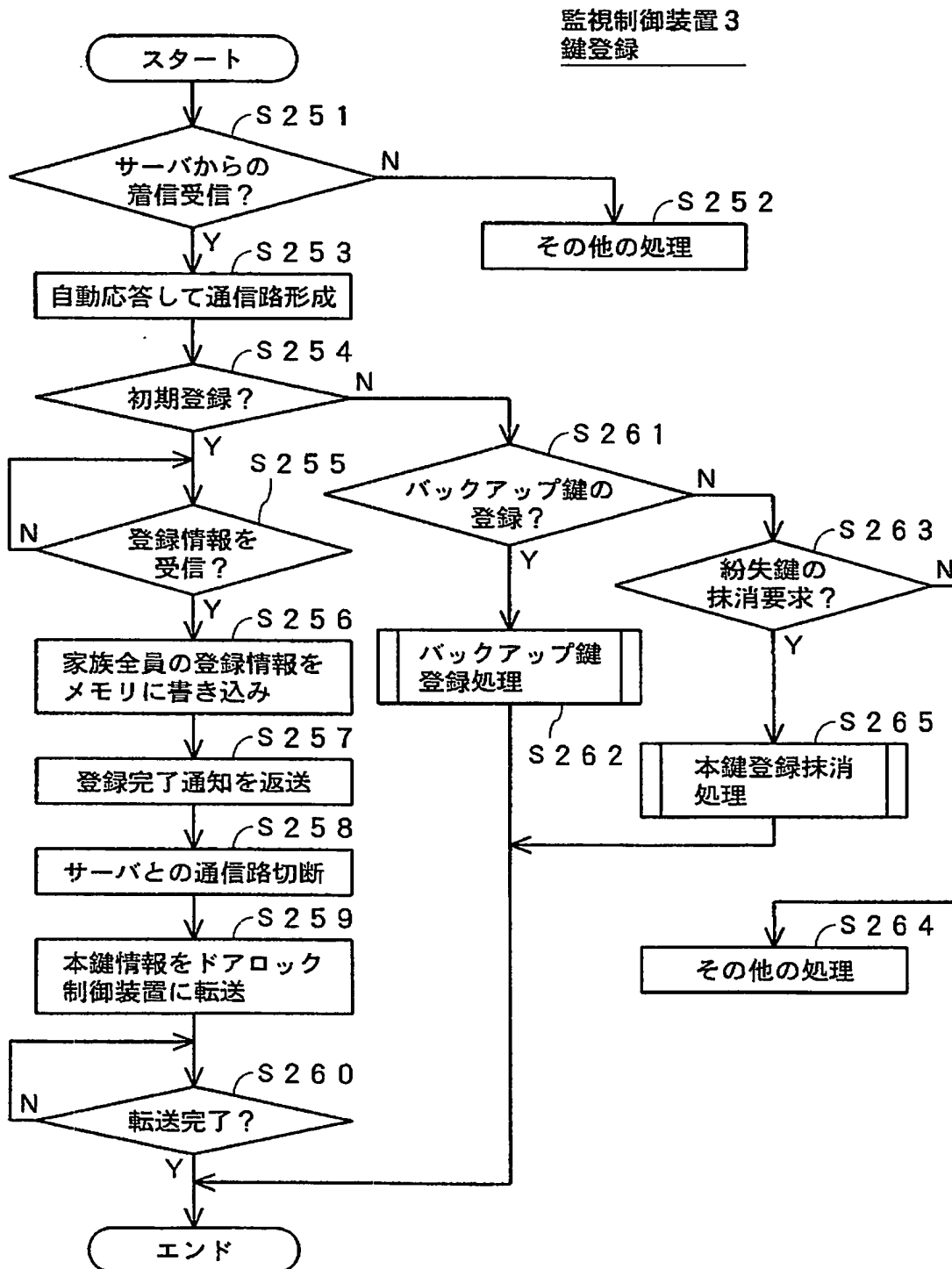
【圖 29】



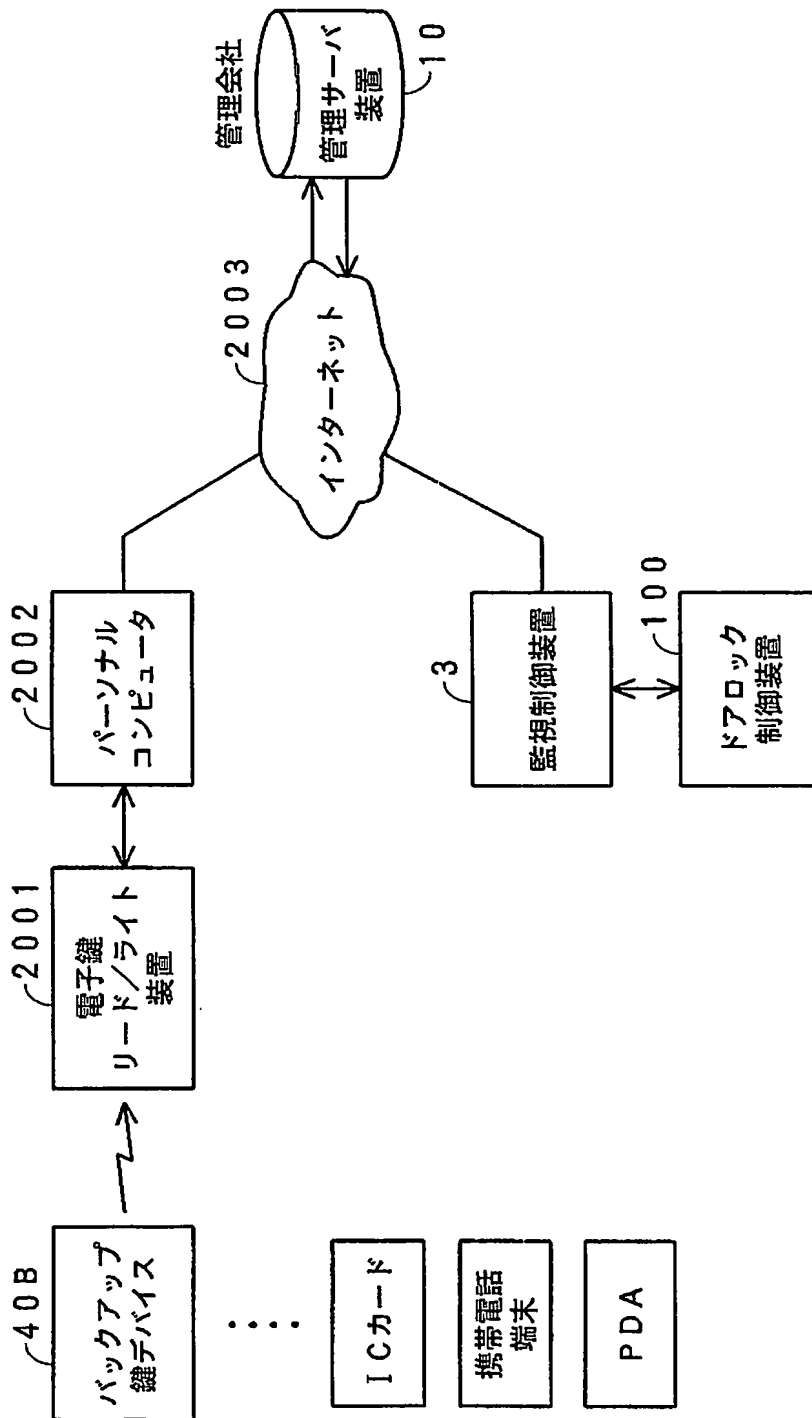
【図 30】

管理サーバ装置 10
初期登録

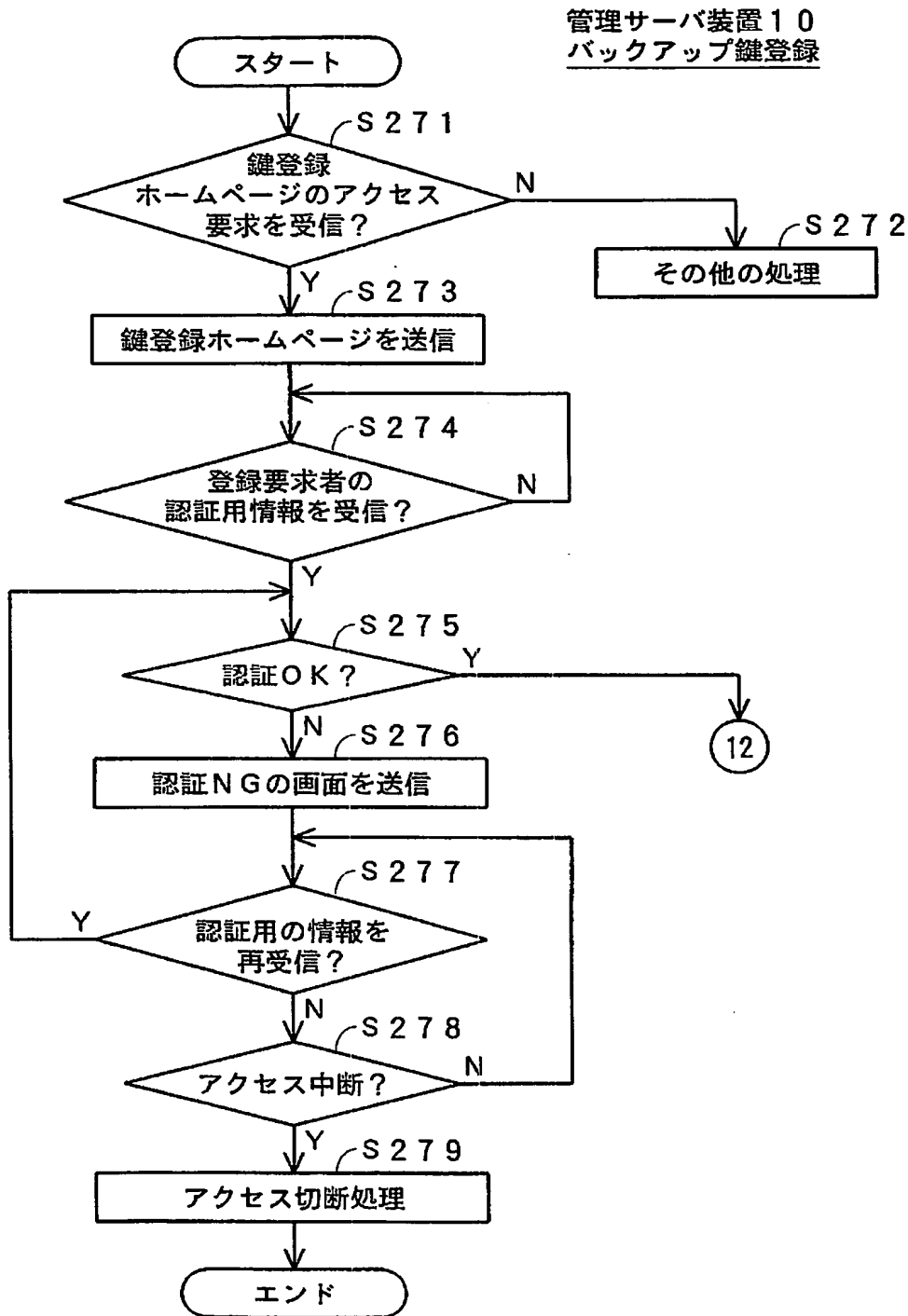
【図 31】



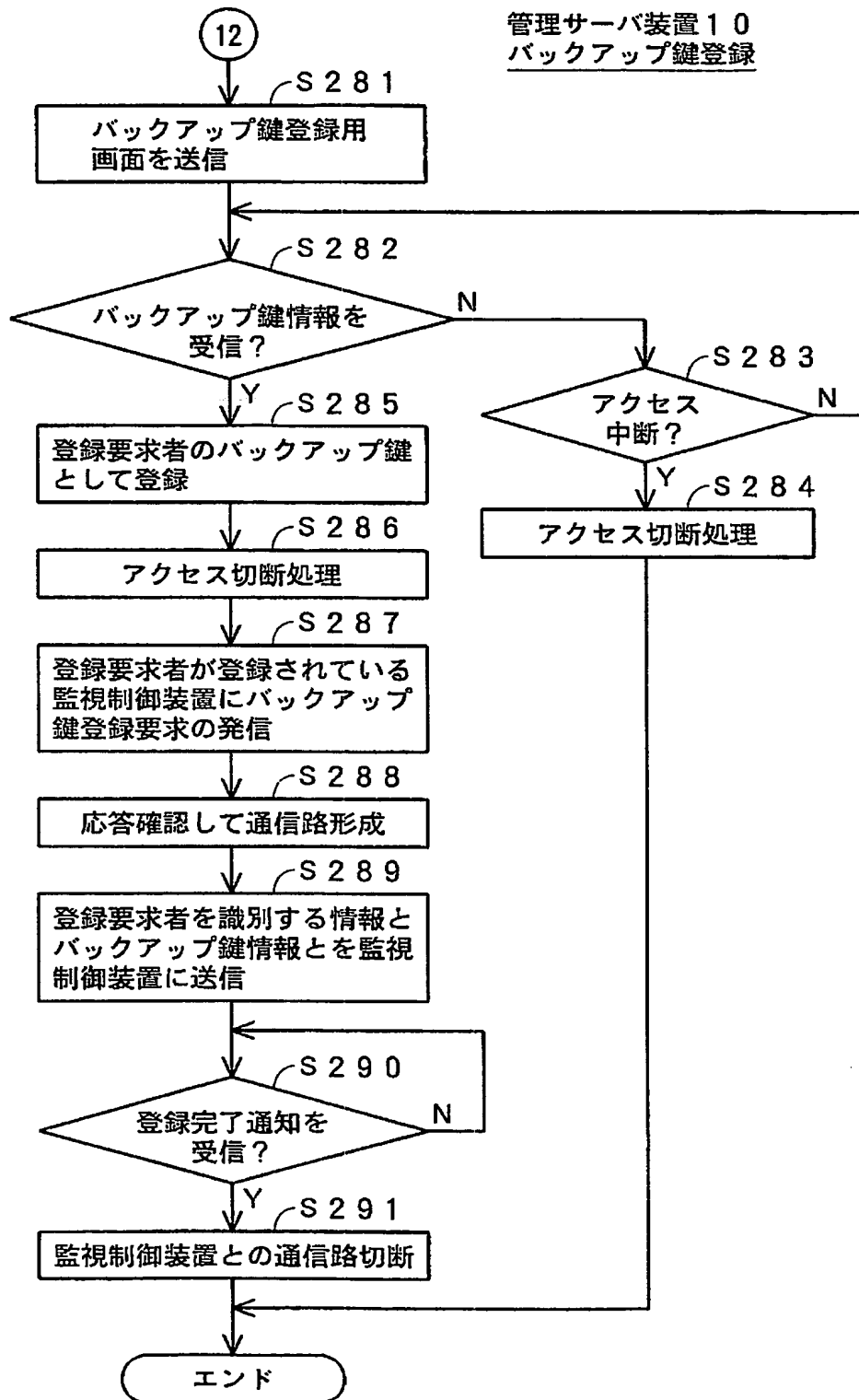
【図 3 2】



【図 33】

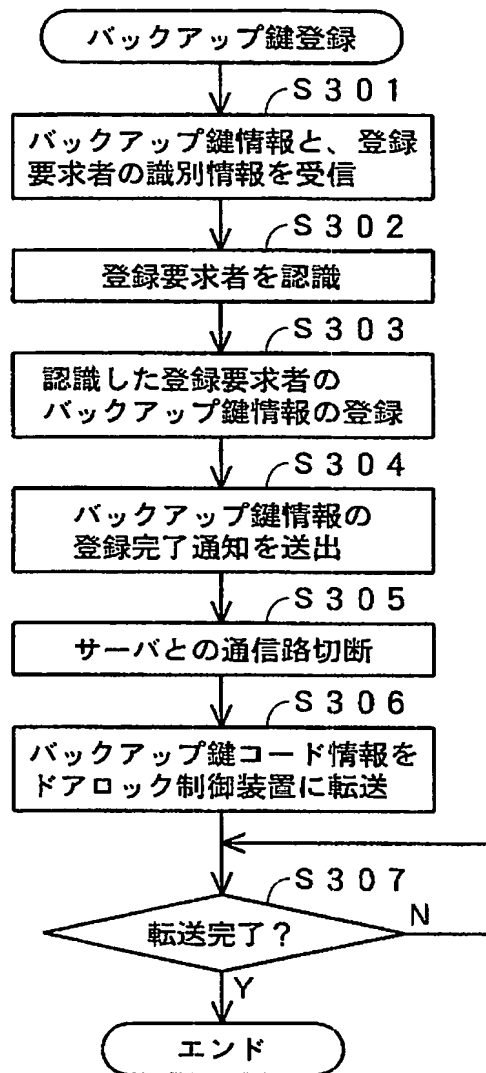


【図 34】

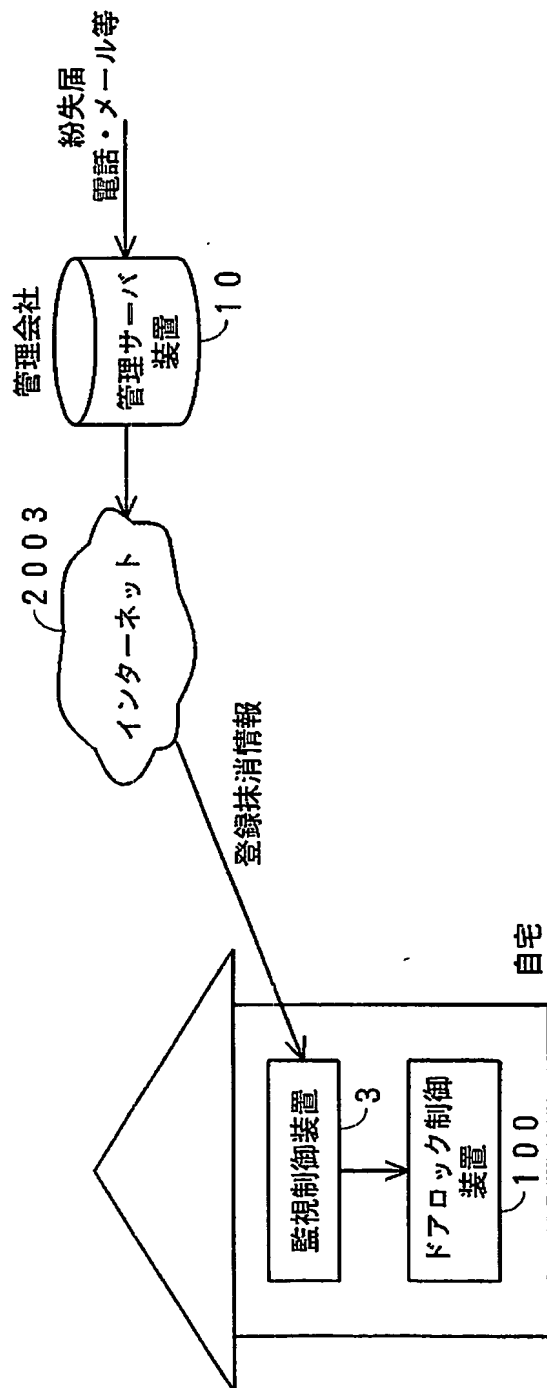


【図 35】

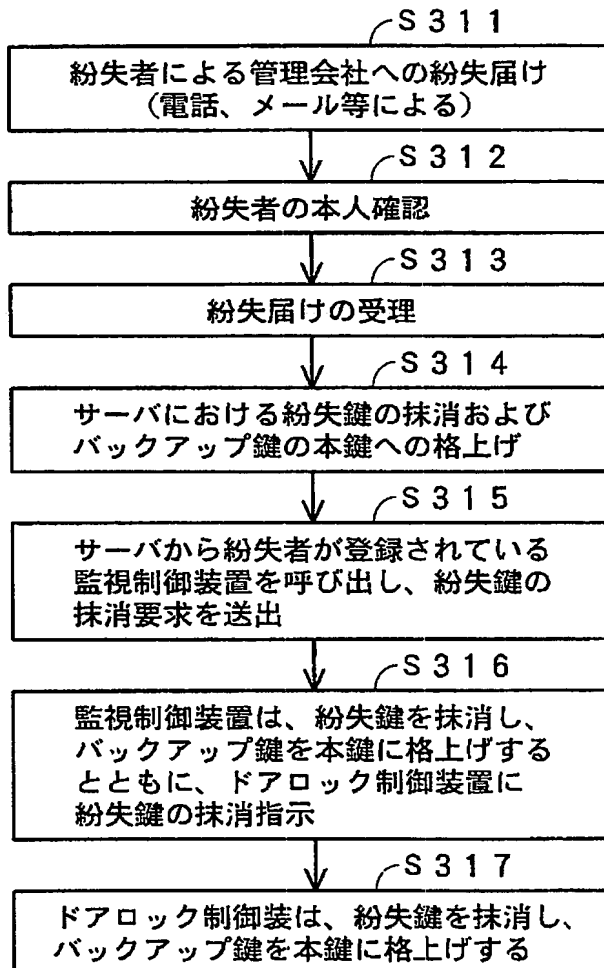
監視制御装置 3
バックアップ鍵登録



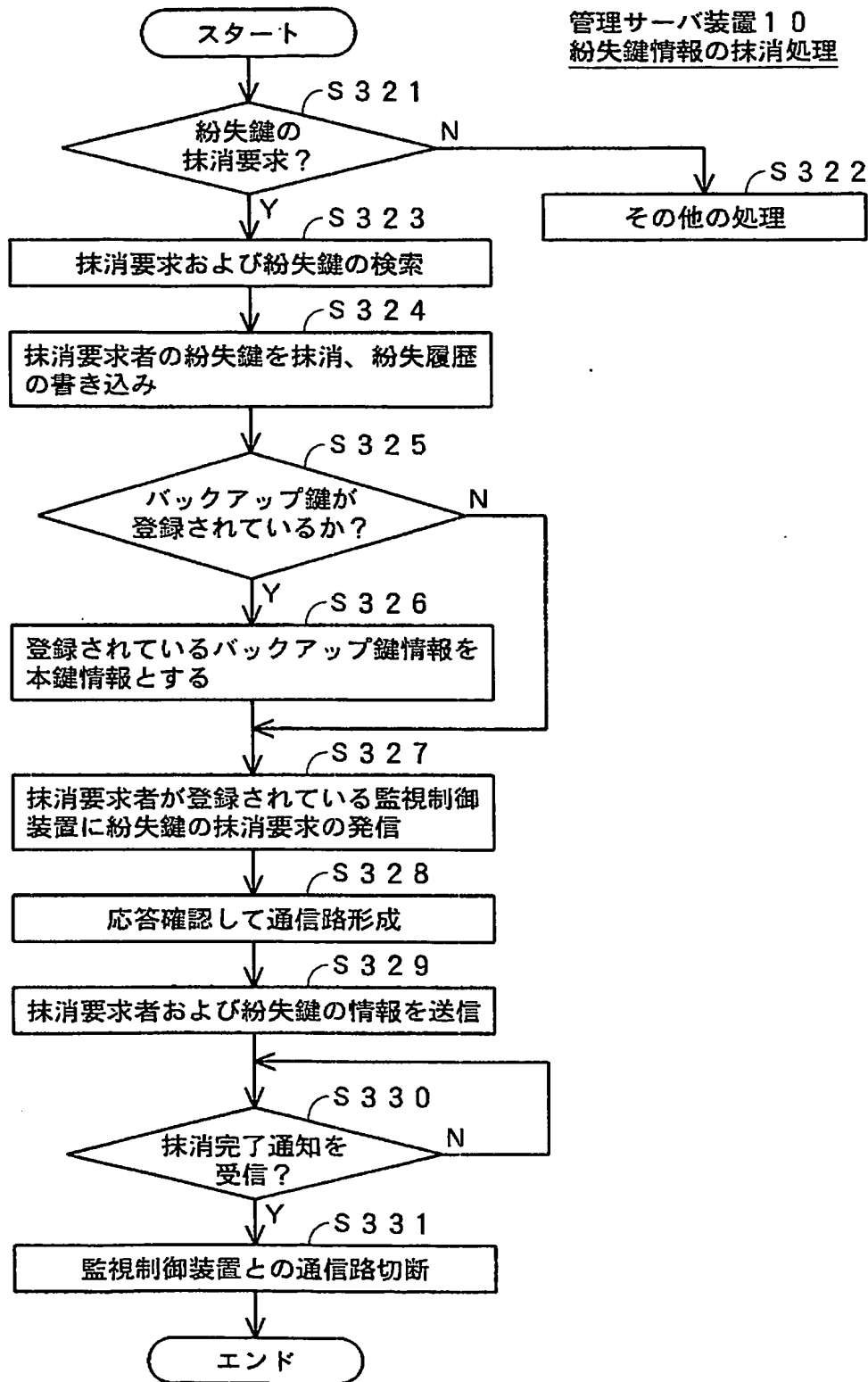
【図 36】



【図 37】

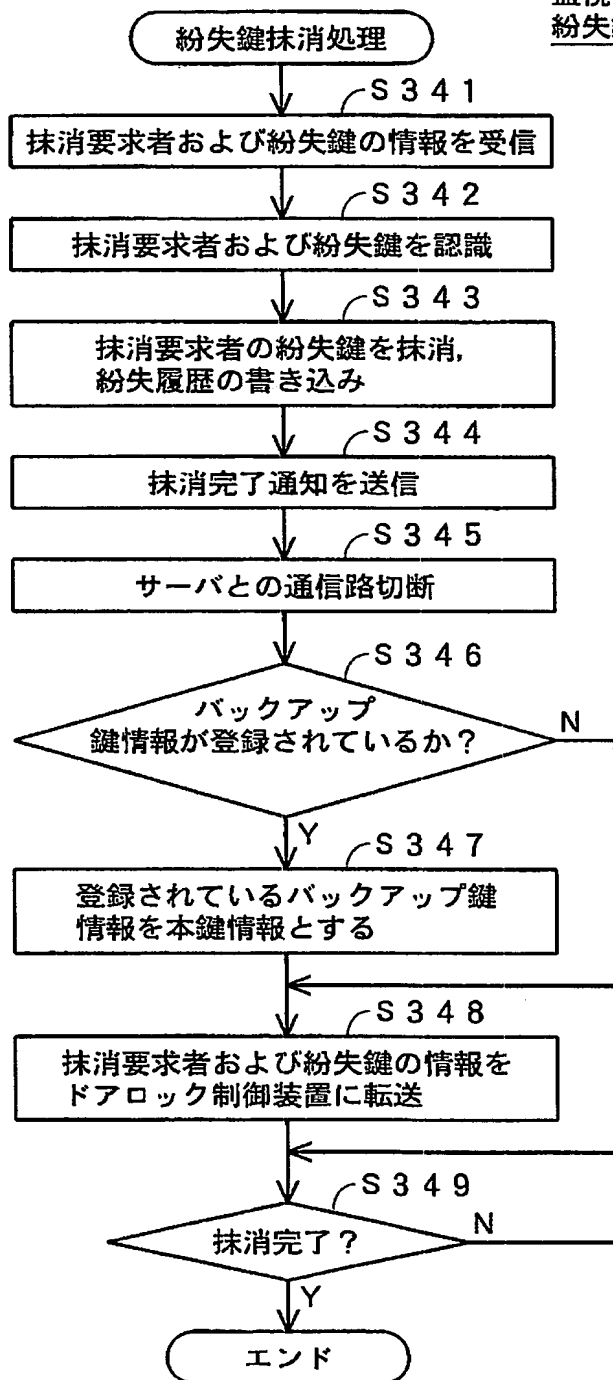
紛失鍵の抹消手順

【図 38】



【図 39】

監視制御装置 3
紛失鍵情報の抹消処理



【書類名】 要約書

【要約】

【課題】 電子鍵管理に関してセキュリティが高い通信システムを提供する。

【解決手段】 電子鍵情報に応じてドアの施錠、開錠を行なうためのドアロック機構を制御する制御装置と、前記制御装置に前記電子鍵情報を送信する通信装置とからなる通信システムである。通信装置は、同一のものが存在しないように一元管理されて割り振られた識別情報を記憶する第1の記憶部を備え、第1の通信部を介して、第1の記憶部の識別情報を、ドアの施錠、開錠を制御するための電子鍵情報として制御装置に送信する。制御装置は、電子鍵情報としての識別情報を記憶する第2の記憶部と、第2の記憶部に識別情報を電子鍵情報として登録するための登録手段と、第2の通信部を通じて通信装置から受信した識別情報と、第2の記憶部に記憶されている識別情報とを比較し、その比較結果に基づいてドアの施錠、開錠を制御する第2の制御部とを備える。

【選択図】 図1

特願 2002-278436

出 願 人 履 歴 情 報

識別番号

[000002185]

1. 変更年月日

1990年 8月30日

[変更理由]

新規登録

住 所

東京都品川区北品川6丁目7番35号

氏 名

ソニー株式会社

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☒ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.